WWW.INFOPULSAS.LT / info@infopulsas.lt

MB CONNECT LINE

remote maintenance solutions

mbNET®

HANDBOOK

MB Connect Line GmbH ● Raiffeisenstraße 4 ● D-74360 Ilsfeld● Telephone +49 (0)7062/9178788 ● Fax +49 (0)7062/9178792● Hot line +49 (0)9851/582529-0

Copyright © MB Connect Line GmbH 2008

No part of this document and its contents may be reproduced, used or distributed without the express permission of MB Connect Line GmbH. Damages will be claimed in the event of infringement. All rights reserved.

These operating instructions cover the functions and application of
the mbNET router

We have aimed to provide the best possible description of the devices and functions. However, we cannot be held liable for the accuracy of the information. The most up to date information is available from our website. We welcome any comments or suggestions for improvement.

Trademarks
The use of any trademark not listed herein is not an indication that it is freely available for use.

MB Connect Line confirms that the mbNET device (MDH6xx/MDH8xx) complies with the basic requirements and overall provisions of European Directive 1999/5/EG. To see the Declaration of Conformity, visit: http://www.mbconnectline.de/support.htm

Issued by:
MB Connect Line Remote Maintenance Solutions GmbH
Raiffeisenstraße 4
74360 Ilsfeld, Germany

Tel.: +49 (0)7062 9178788
Fax: +49 (0)7062 9178792
Technical support: +49 (0)9851 582529-0
E-Mail: info@mbconnectline.de
Website: www.mbconnectline.de

Table of contents

1. Introduction ... 8

1.1 Brief description ... 8

1.2 Features ... 8

2. Safety instructions ... 9

3. Technical data ... 10

4. What is included in the package ... 11

5. Displays, controls and connections ... 12

5.1 Front panel view ... 12

5.2 Top, bottom and back panel views ... 14

6. Interfaces ... 15

6.1 Pin assignment ... 15

6.1.1 Pinout of top panel terminal blocks X1 and X2 ... 15
6.1.2 Pinout of bottom panel RJ12 jack ... 15
6.1.3 Pinout of front panel serial interfaces COM1 and COM2 ... 15
6.1.4 Pinout of front panel LAN / WAN ports ... 16
6.1.5 Pinout of front panel USB port ... 16

7. First time operation ... 17

7.1 Connecting the router to the power supply and switching on ... 17

7.1.1 Connecting the router to a configuration PC ... 18

7.2 Configuration prerequisites ... 19

7.2.1 How to set computer address (IP address) and subnet mask in XP ... 20

7.3 Initial configuration ... 21

8. Basic configuration of the router using the web interface ... 22

8.1 Web interface home page ... 22

8.2 Icons, buttons and fields ... 23

8.3 System settings ... 25

8.4 Security Settings ... 27

8.4.1 Save Settings ... 28

9. Connection Scenarios ... 29

9.1 General ... 29

9.2 Configuring the industrial router for connection over the telephone network ... 31

9.2.1 Connecting and configuring the router ... 32
9.2.1.1 Connecting the router ... 32
9.2.1.2 Configuring the router using the web interface ... 33
9.2.2 Configuring a client (PC) to access the router ... 37
9.2.3 Establishing a connection between the client PC and the industrial router ... 39
9.2.4 Displaying and verifying connection status ... 39

9.3 Configuring the industrial router for connection via the Internet ... 40

9.3.1 Connecting and configuring the router ... 41
9.3.1.1 Connecting the router ... 41
9.3.1.2 Configuring the router using the web interface ... 42
9.3.2 Router Internet dial-in ... 46
9.3.3 Displaying the Internet connection ... 46

9.4 Configuring the industrial router for connection to the Internet using a DSL modem ... 47

9.4.1 Connecting and configuring the router ... 47
9.4.1.1 Connecting the router ... 47
9.4.1.2 Configuring the router using the web interface ... 48
9.4.2 Establishing a connection between client PC and router ... 51
9.4.3 Displaying connection status ... 52

9.5 Configuring the industrial router for connection to the Internet via an existing router ... 53

9.5.1 Connecting and configuring the router ... 54
9.5.1.1 Connecting the router ... 54

9.5.1.2 Configuring the router using the web interface 55
9.6 Configuring the industrial router for VPN connection to a client 58
9.6.1 Connecting and configuring the router 59
9.6.1.1 Connecting the router 59
9.6.1.2 Adding VPN dial-in users 59
9.6.1.3 Configuring the router (VPN server) 60
9.6.2 Configuring a client PC for a VPN connection to the router 64
9.6.3 Setting up a VPN connection between client PC and router 66
9.6.3.1 Router Internet dial-in 66
9.6.3.2 Setting up a VPN connection from client to router 66
9.6.3.3 Additional settings 66
9.7 Configuring a connection between two routers via VPN PPTP 67
9.7.1 Settings for connecting two industrial routers – PPTP – server 68
9.7.2 Settings for connecting two industrial routers – PPTP – Clients 70
10. Creating certificates and revocation lists using XCA. 73
10.1 Certificates overview 73
10.2 Creating certificates 74
10.2.1 Creating a root certificate 74
10.2.1.1 Root certificate source 75
10.2.1.2 Root certificate subject 76
10.2.1.3 Root certificate extensions 77
10.2.1.4 Root certificate key usage 79
10.2.2 Creating a client certificate 80
10.2.2.1 Client certificate source 81
10.2.2.2 Client certificate subject 83
10.2.2.3 Client certificate – Extensions 84
10.2.2.4 Client certificate – Key usage 85
10.2.2.5 Client certificate – Netscape 85
10.3 Creating CRL files (revocation lists) 88
11. Importing certificates in Windows XP 90
12. System Settings 93
12.1 System – WEB 93
12.2 System – Users 94
12.2.1 General 94
12.2.2 Editing users 94
12.2.3 Adding users 95
12.2.4 Deleting Users 97
12.3 System – Certificates 98
12.3.1 Personal Certificates 99
12.3.2 Root certificate (CA) 100
12.3.3 Peer certificates (IPSec) 101
12.3.4 CRL 101
12.4 System – USB 102
12.5 System – Logging 103
12.6 System – Configuration 105
12.7 System – Firmware 106
13. Network 108
13.1 Network – LAN 108
13.2 Network – WAN 109
13.3 Network – Modem 110
13.3.1 Network – Modem – Incoming 110
13.3.2 Network – Modem – Outgoing 113
13.3.3 SMS menu settings 116
13.3.4 Network – Modem – Callback 117
13.3.5 Network – Modem – SMS 118
13.3.6 Remote service control commands using SMS 118
13.4 Network – Internet 119
13.4.1 Network – Internet – Internet Connections 119

13.4.2 Network – Internet – Internet Settings ... 120
13.4.3 Internet failover connection ... 121
13.5 Network – DHCP ... 125
13.6 Network – DNS server ... 126
13.7 Network – Hosts ... 127
13.8 Network – DynDNS ... 128
13.8.1 General ... 128
13.8.2 How to set up DynDNS configuration ... 128
14. Serial interfaces ... 131
14.1 General ... 131
14.1.1 RS232/485 serial interfaces ... 131
14.1.2 MPI/PROFIBUS interface ... 134
14.1.3 Settings for Simatic Manager ... 137
14.2 Enabling RFC1006 on the mbNET ... 137
14.2.1 Settings for NETPro Step 7 ... 138
14.2.2 Create subnets ... 138
14.2.3 Add PC station ... 139
14.2.4 Configure PC station ... 140
14.2.5 Add PC/PG station ... 141
14.2.6 Configure mbNET PC station ... 144
14.3 Connecting to S7 using the mbNET S7 driver ... 147
15. Security settings ... 150
15.1 General ... 150
15.2 WAN>LAN ... 151
15.3 LAN>WAN ... 152
15.4 Forwarding ... 154
15.5 NAT ... 155
16. VPN-IPSec ... 156
16.1 Configuring a VPN-IPSec connection with two routers ... 156
16.1.1 Connection settings ... 157
16.1.2 Network Settings ... 158
16.1.3 Authentication ... 158
16.1.4 Protocol options ... 162
16.1.5 L2TP Server Configuration ... 163
17. VPN-PPTP ... 164
17.1 Server settings ... 164
17.2 Client setting ... 166
18. VPN – OpenVPN ... 167
18.1 Basics about OpenVPN ... 167
18.2 Connection scenarios ... 168
18.2.1 Client – router ... 168
18.2.1.1 No authentication or static key ... 170
18.2.1.2 Authentication with certificates ... 170
18.2.1.3 Configuring an OpenVPN Windows client ... 171
18.2.1.3.1 No authentication ... 172
18.2.1.3.2 Authenticating a Windows client with static key ... 173
18.2.1.3.3 Starting the OpenVPN connection ... 174
18.2.2 Router – router ... 174
18.2.2.1 Server – no authentication or static key ... 176
18.2.2.2 Server – authentication with certificates ... 176
18.2.2.2.1 Single client: Only one client can dial in ... 177
18.2.2.2.2 Multi client: Multiple clients can dial in ... 177
18.2.2.3 Client authentication: No or static key ... 179
18.2.2.4 Client authentication: With certificates ... 180
18.2.3 Authentication ... 181
18.2.3.1 No authentication ... 181
18.2.3.2 Authentication with static key ... 181

18.2.3.2.1 **Key management** ... 182
18.2.3.3 Authentication with certificates ... 183
18.2.3.3.1 **Authentication with CA certificate and own certificate** ... 183
18.2.3.3.2 **Authentication with CA certificate and own certificate and user/password** ... 184
18.2.3.3.3 **Server** ... 184
18.2.3.3.4 **Client** ... 185
18.3 Inactivity settings ... 187
18.4 Protocol options ... 188
19. I/O Manager ... 191
19.1 Configuring the connection ... 192
19.1.1 Creating the PLC connection ... 193
19.1.2 Creating the tags ... 194
19.2 Configuring the logging function ... 195
20. Alarm management ... 197
20.1 General ... 197
20.2 Digital inputs ... 197
20.2.1 Multiplex inputs ... 198
20.3 Digital outputs ... 201
21. Status messages ... 202
21.1 General ... 202
21.2 Status – Interfaces ... 202
21.3 Status – Network ... 203
21.4 Status – Modem ... 204
21.5 Status – Internet ... 206
21.6 Status – DHCP ... 208
21.7 Status – DNS Server ... 209
21.8 Status – DynDNS ... 210
21.9 Status – NTP ... 211
21.10 Status – VPN-IPSEC ... 212
21.11 Status – VPN-PPTP ... 213
21.12 Status – VPN OpenVPN ... 214
21.13 Status – Diagnostics ... 215
21.14 Status – USB ... 216
21.15 Status – Alarmmanagement ... 217
21.16 Status – System ... 218
22. Factory settings on delivery ... 220
22.1 Username and password ... 220
22.2 IP address of the router ... 220
23. Loading the factory settings ... 220
24. Initializing the modem ... 221
General information on the AT commands ... 221
24.1 Analog modem commands ... 221
24.2 ISDN terminal adapter (TA) commands ... 223
25. Appendix ... 224
25.1 Country codes for analog devices ... 224
26. Index ... 229

1. Introduction

1.1 Brief description

The *mbNET* industrial router offers you optimum flexibility and security, making remote communication with your systems both easy and secure. Thanks to its compact design, the *mbNET* router will fit into any switch cabinet, and with its multiple interfaces and drivers, is the perfect solution for integrating different control systems.
The *mbNET* router is configurable using a web interface.

1.2 Features

- Fully configurable using web interface via locally connected computer, or remotely.
- Deployable worldwide using different modem connections, (ISDN, analog, mobile broadband) plus access via LAN and Internet.
- Secure connection using an integrated firewall with IP filter, NAT and port forwarding, VPN with AES, DES/3DES/DESX, Blowfish or RC2 encryption, and authentication via pre-shared key (PSK), static key or certificate (X.509).
- Alarm management:
  - fully configurable digital inputs and outputs, and the ability to send via email, SMS or Internet dial-up
  - via remote output switching in the event of a fault or with an active Internet connection.
- Integrated server secures all settings, keys and certificates and allows data sharing within the network via connected USB flash or hard drive.
- Variable RS232, RS485, RS422 RS interface or optional MPI/PROFIBUS for connecting control systems.

2. Safety instructions

- The router is built to the latest technological standards and recognized safety standards (see Declaration of Conformity).
- The router must be installed in a dry location. No liquid must be allowed to get inside the router, as this could result in electric shocks or short circuits.
- The router is for indoor use only.
- Never open the router chassis. Unauthorized opening and improper repair can pose a danger to the user. Unauthorized modifications are not covered by the manufacturer's warranty.
  Opening up the device voids the warranty.
- The router must be disposed of in line with European regulations and German legislation on electronics and electronic device, and not as general household waste.

3. Technical data

Voltage V (DC)	10 – 30V
Power consumption	Max. 300mA at 24V
Digital inputs	4 digital inputs (10-30V) (fuse-protected)
Digital outputs	2 digital outputs (200mA max. / output)
IP protection class	20
Area of application	Dry environments
Operating temperature	0...50°C
Storage temperature	-20...+60°C
Weight	Approx. 650 g
Humidity	0...95% (non-condensing)
Dimensions (max.)	124 mm x 48 mm x 124 mm (H x W x D)
Interfaces	RS232/485, RS422, MPI/PROFIBUS, LAN 10/100 Mbit/s, dependent on device
General license	EN 61000-6-4:2001, interference emissions for industrial environments EN 61000-6-2:2001, interference immunity for industrial environments

4. What is included in the package

First, check that the following parts are in the product package:

- ❑ ***mbNET* router**

Figure 1: *mbNET router*

- ❑ **Straight-through Ethernet cable**

Figure 2: Straight-through Ethernet cable

- ❑ **Router variants with analog modem: RJ10-RJ10 cable, and RJ10 to TAE adapter**
- ❑ **For router variants with ISDN modem: RJ10-RJ45 cable**

Figure 3: analog connection cable

Figure 4: IDSN connection cable

- ❑ **For router variants with GSM modem: GSM antenna**

Figure 5: GSM antenna

- ❑ **Quick Start Guide**

Figure 7: Quick Start Guide

If any of these parts are missing or damaged, please contact:

MB CONNECT LINE GMBH
Winnettener Straße 5
D-91550 Dinkelsbühl
Tel.: +49 (0)9851 582529-0
Fax: +49 (0)9851 582529-99
E-Mail: info@mbconnectline.de
Website: www.mbconnectline.de

Keep the box and the original packaging in case you may have to send the device for repair at a later date.

5. Displays, controls and connections

5.1 Front panel view

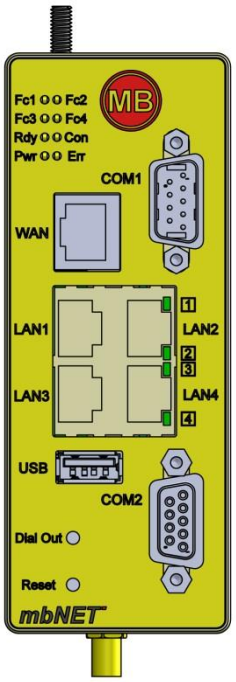


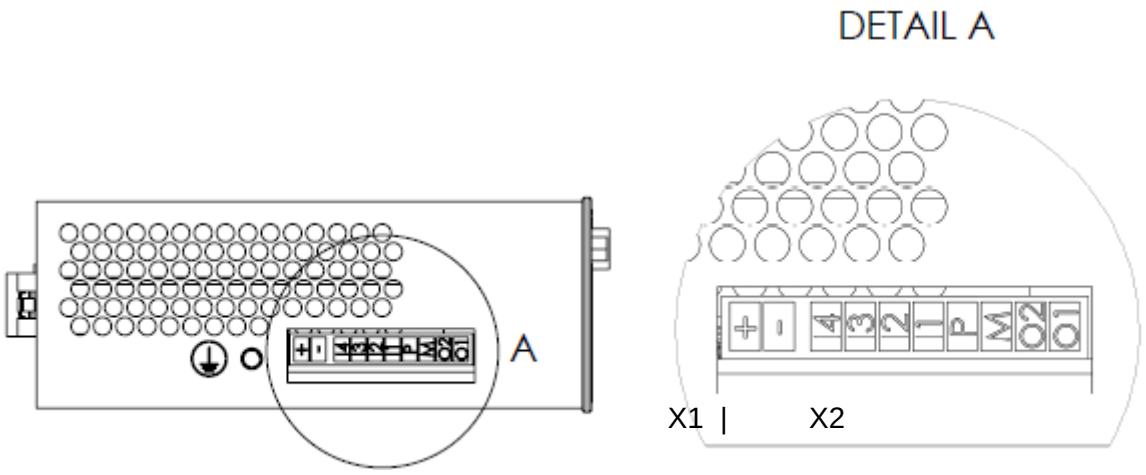
Figure 6

Label	Status	Description
Pwr (Power)	LED off	Router power source is switched off or router is not connected to power source / power pack.
	LED on	Power source is connected to terminal block and switched on.
Rdy (Ready)	LED flashing	The Ready LED does this for approx. 35 seconds when the device is switched on. After this, flashing indicates boot sequence. This may take up to 90 seconds depending on the type of device.
	LED solid	The router is ready
Fc1 (Function 1)	LED off	Serial interface COM1 not receiving data.
	LED on	Serial interface COM1 receiving data.
Fc2 (Function 2)	LED off	Serial interface COM1 not sending data.
	LED flashing	Serial interface COM1 sending data.
Fc3 (Function 3)	LED off	Serial interface COM2 not receiving data.
	LED flashing	Serial interface COM2 receiving data. On if MPI: bus communication OK
Fc4 (Function 4)	LED off	Serial interface COM2 not sending data.
	LED flashing	Serial interface COM2 sending data. If MPI: bus transferring data
Con (Connect)	LED off	No connection to Internet or VPN
	LED on	Connection to Internet
	LED flashing (1.5Hz)	VPN connection active
	LED flashing (3 Hz)	Internet or VPN connection is being established
Err (Error)	LED off	Router working without errors
	LED on	Router error. Diagnostics under System Status(see **Status – System**)

Label	Status	Description
WAN	-	Router WAN port. (customer network, DSL modem ...)
WAN LED	LED green	Network connection available.
WAN LED	LED flashing orange	Network data transfer active.
LAN1 – 4		Local network ports (e.g. machine network)
LAN LED1 – 4 (Dual LED)	LED green	Network connection available.
	LED flashing orange	Network data transfer active.
USB	-	Portable USB drive port.
Dial out	-	This button establishes an Internet or VPN connection.
Reset	-	Pushing this button restarts the router (so-called cold start).
COM1		COM1 port for connecting to devices with RS232 / RS485, RS422 interface
COM2	-	COM2 port for connecting to devices with MPI interface

5.2 Top, bottom and back panel views

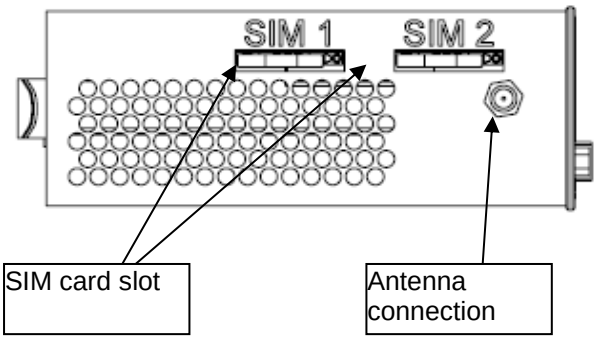
Top



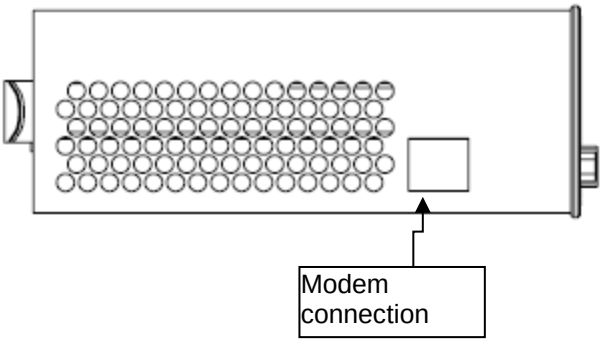
X1	**+**	Power supply connection 10-30V DC
	-	0V DC connection
X2	**4**	Digital input I4 (10-30V)
	3	Digital input I3 (10-30V)
	2	Digital input I2 (10-30V)
	1	Digital input I1 (10-30V)
	P	Fuse-protection 10-30V DC
	M	0V DC connection
	O2	Digital output A2
	O1	Digital output A1

Bottom

GSM/UMTS variant



Analog/ISDN modem variant



6. Interfaces

6.1 Pin assignment

6.1.1 Pinout of top panel terminal blocks X1 and X2

X1	**+**	Power supply connection 10-30V DC
	-	0V DC connection
X2	**1**	Digital input I1 (10-30V)
	2	Digital input I2 (10-30V)
	3	Digital input I3 (10-30V)
	4	Digital input I4 (10-30V)
	P	Fuse protection 10-30V DC
	M	0V DC connection
	02	Digital output A2
	01	Digital output A1

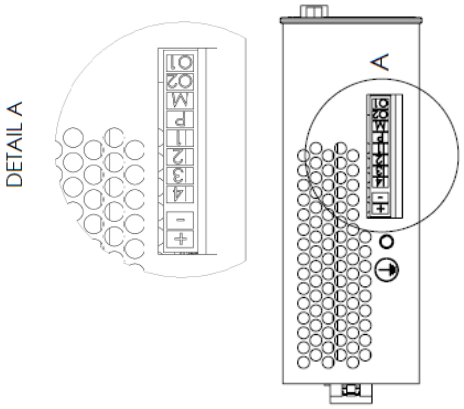


Figure 7

6.1.2 Pinout of bottom panel RJ12 jack

Pin	ISDN	Analog
1	Not Connected	Not Connected
2	TX+	Not Connected
3	RX+	Lb/b
4	RX-	La/a
5	TX-	Not Connected
6	Not Connected	Not Connected

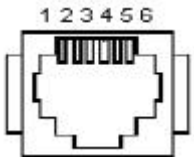


Figure 8

6.1.3 Pinout of front panel serial interfaces COM1 and COM2

Pin	RS 232	RS 485	MPI
1	DCD Data Carrier Detect	Not Connected	Not Connected
2	RxD Receive Data	RxD – Receive Data	GND 24V
3	TxD Transmit	TxD + Transmit Data	Data circuit B
4	DTR Data Terminal Ready	+5Volts (only in 4-wire operation)	Send request
5	Ground signal	Ground signal	GND 5V(200mA)
6	DSR Data Set Ready	Not Connected	5V output
7	RTS Request to Send	TxD – Transmit Data	24V supply input
8	CTS Clear to Send	RxD+ Receive Data	Data circuit A
9	RI Ring Indicator	Not Connected	Send request

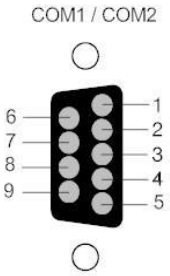


Figure 9

6.1.4 Pinout of front panel LAN / WAN ports

	Signal
1	TX+
2	TX-
3	RX+
4	Not Connected
5	Not Connected
6	RX-

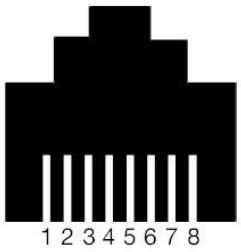


Figure 10

6.1.5 Pinout of front panel USB port

	Signal
1	VCC (+5V)
2	- Data
3	+Data
4	GND

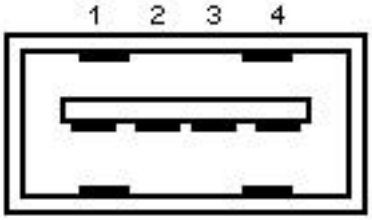



Figure 11

7. First time operation

7.1 Connecting the router to the power supply and switching on

The router is designed for installation in switch cabinets. The device is designed for mounting on top-hat rails (based on DIN EN 50022).

Please note
Before connecting the router to a network or PC, first ensure that it is properly connected to a power supply, otherwise it may cause damage to other equipment. You should therefore follow the instructions given below

IMPORTANT
Connect equipotential bonding to the grounding lug on the router's top panel.

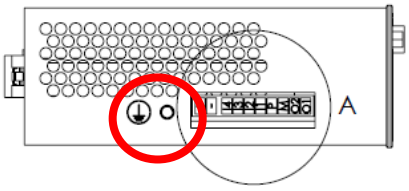
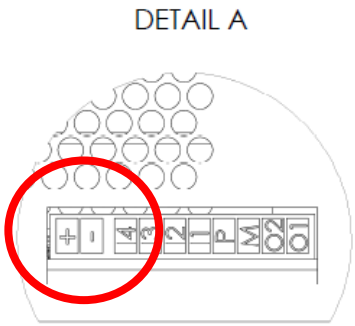


Figure 12



- ❑ Insert the router into the DIN rail. To do this, position the upper guide on the rail and then press the router downwards against the rail until fully inserted.
- ❑ Connect the (10-30V DC) power supply to the **X1 terminal** of the router.

Figure 13

Make sure the polarity is correct.

- ❑ Now switch on the power supply. The green **Power** LED should light up immediately. After approx. 90-110 seconds (depending on device model) the **Ready** LED should be solid. The device is now ready for operation.

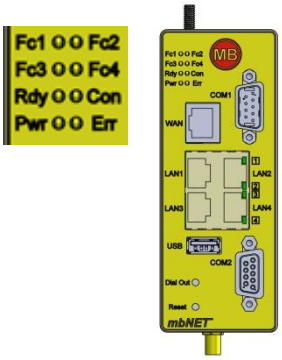


Figure 14

For further support on the mbNET industrial router, visit our online support forum at www.mbconnectline.de

7.1.1 Connecting the router to a configuration PC

- ❑ Before configuring the router, connect it to the computer using the crossover cable supplied (**1**). To do this, connect one end of the cable to the router port labeled **LAN,** and the other end to your computer's network card.

Figure 15

7.2 Configuration prerequisites

To configure the router, you will need:

- ❑ **a PC with a network card**

- ❑ **an Internet browser** (e.g. Mozilla Firefox or Internet Explorer)

- ❑ **The required settings on your PC are as follows:**
  - **the computer's IP address must be set to 192.168.0.X where X is variable**
  - **the subnet mask must be 255.255.255.0**

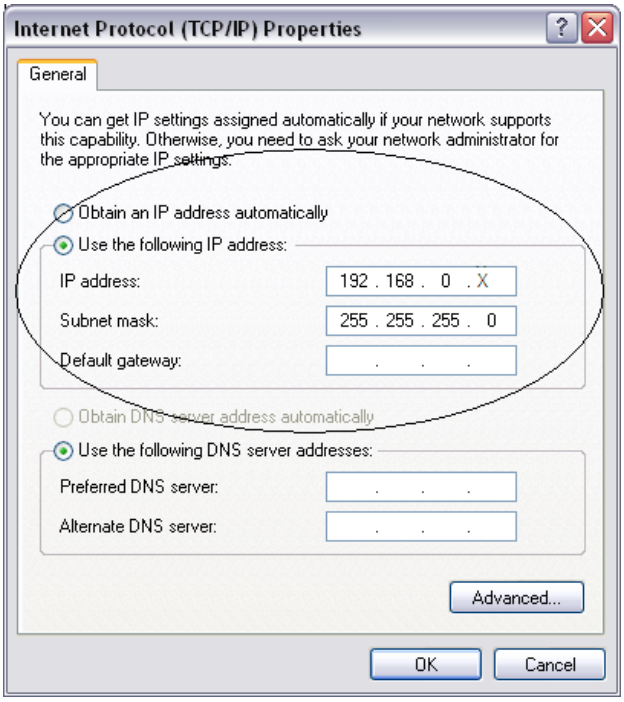

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 0 . X
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Figure 16

For instructions on how to create the required settings on a PC, please see the next page. If you already know how to set the IP address and subnet mask, set them as described above and then proceed with configuration as described in in **Initial Configuration**

7.2.1 How to set computer address (IP address) and subnet mask in XP

To set the IP address, proceed as follows:

- ❑ First, select Control Panel from the Windows Start menu (**1**) and then double-click on Network Connections (**2**).
- ❑ Right-click on **Local Area Connection (3)** and select **Properties.**
- ❑ In the next window, double-click on **Internet Protocol (TCP/IP) (4).**
- ❑ In the next window, enter the appropriate IP address. An appropriate IP address would be e.g. **192.168.0.2**.

Please note:
the Internet IP address must be 192.168.0.X and must not already be in use by another network subscriber.

- ❑ In Subnet mask, enter **255.255.255.0** and in Default gateway, enter the router IP Address as shown in the section on **Router IP Address**.
- ❑ Where a DNS server is in use, there is an option to select "**Obtain DNS server address automatically**".
- ❑ To save and close the settings, click **OK** on each of the open windows.

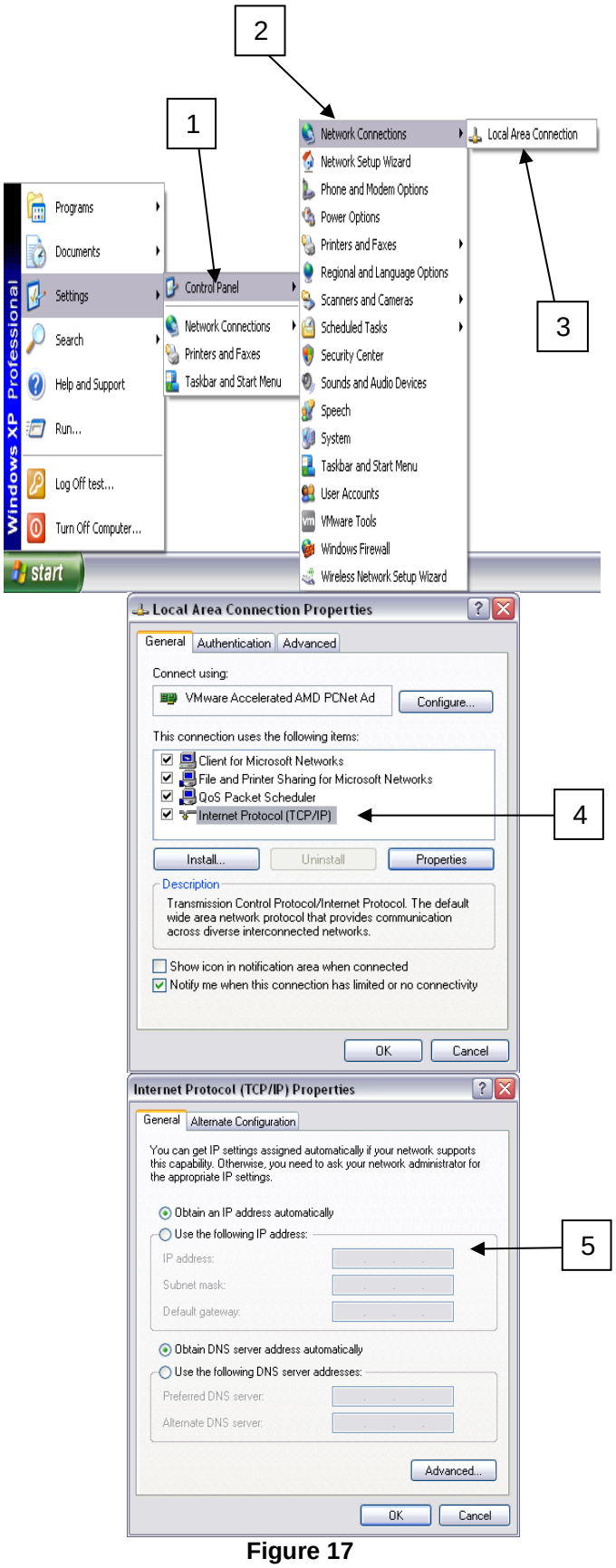


Figure 17

7.3 Initial configuration

Proceed as follows:
Open your browser and enter the router's IP address in the address bar.

The factory setting is: 192.168.0.100

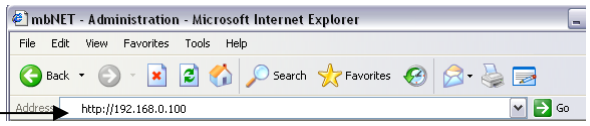


Figure 18

Log into the router using the following settings:

- ☐ User name: admin
- ☐ Password: no password required

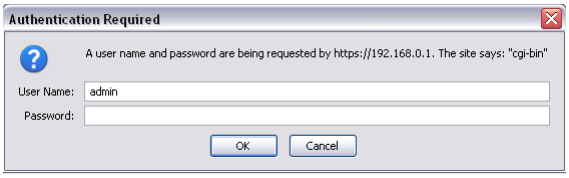


Figure 19

Firmware versions lower than 1.2.0

On successful log in you will be taken to the **configuration interface home page** (see screenshot, right).

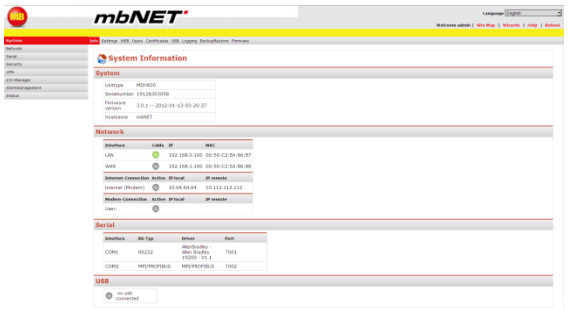


Figure 20

With **firmware versions 1.2.0 and higher** a connection wizard will launch, simplifying network, Internet and VPN connection set up. The wizard is easy to use and takes you through the configuration process step by step.
You can also launch the wizard manually. To do this, click on "Wizards" at the top right of your browser window.

Figure 21

8. Basic configuration of the router using the web interface

8.1 Web interface home page

The home page is designed to provide you with an at-a-glance view of the most important information on *mbNET* router access or status. The side (**1**) and top (**2**) navigation bars will provide the support you need when configuring the router. The navigation bar at the top (**2**) displays the submenu for each of the main menu items listed in the navigation bar at the side (**1**).

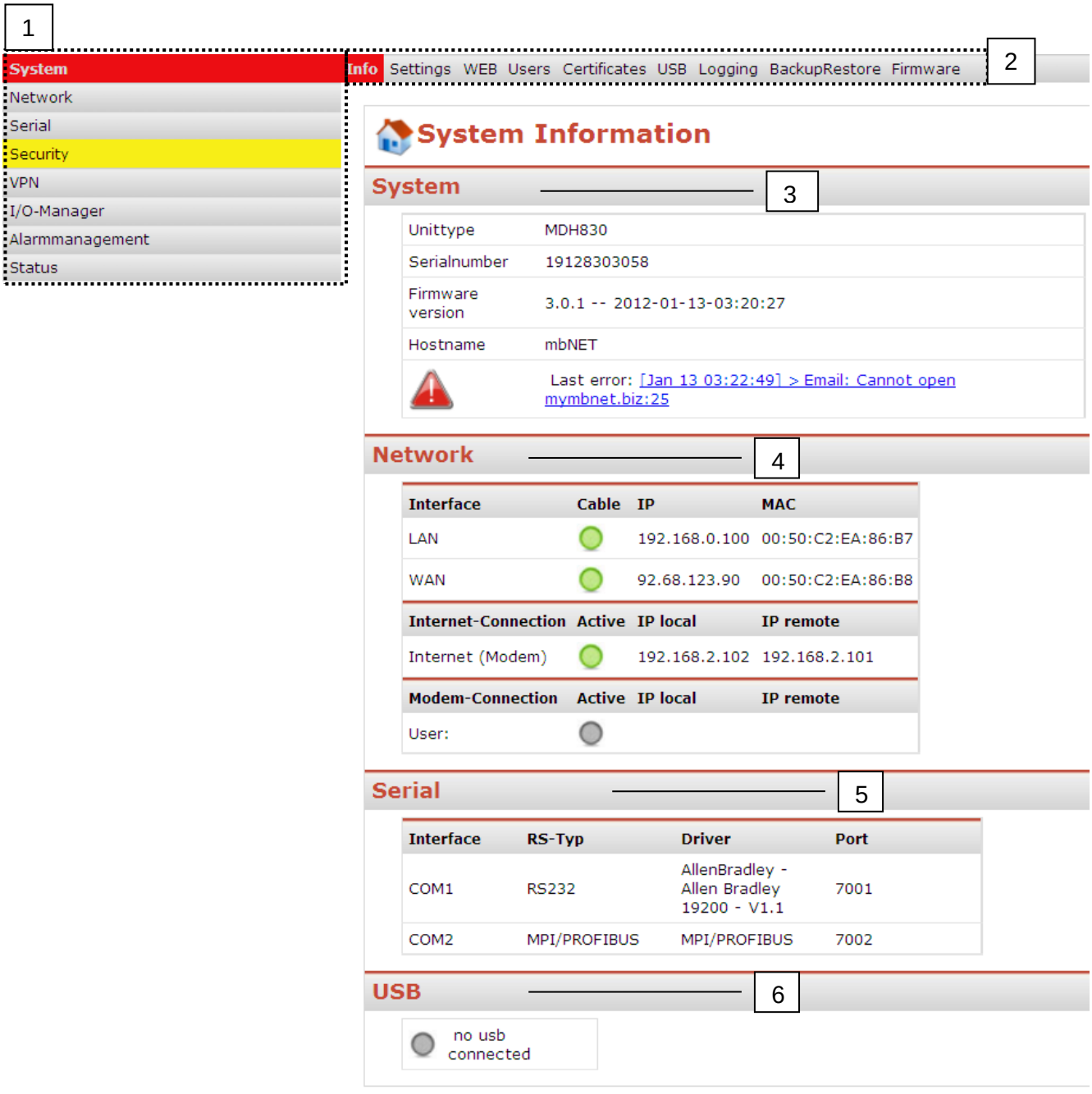


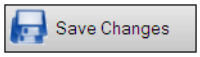
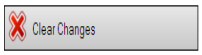
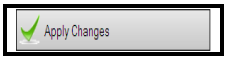
Figure 22

Item	Label	Function
3	System	System information such as device model, device name, current firmware version and serial number of the router.
4	Network	**Interface: LAN – WAN:** Displays which network connections are currently connected to the existing network via the respective ports. A green icon indicates an existing connection. **Internet connection:** A currently active Internet connection (or connections) is indicated by a green dot. If there is no currently active Internet connection, the circle is solid gray. **Modem connection:** Only **incoming** modem connections are shown here. A green dot means that a modem connection is established. The display also shows which user is connected to the modem.
5	Serial	This shows the current configuration of interfaces **COM1** and**COM2**.
6	USB	Information on connected USB storage devices. A connected storage device (e.g. flash drive or external hard drive) is indicated by a green dot.

Basic configuration of the router using the web interface

8.2 Icons, buttons and fields

In the rest of these operating instructions you will repeatedly encounter specific icons. These are listed and explained on the next page.

No.	Icon and field types	Description
1		**Gray LED:** connection inactive / cable or USB device disconnected. / **Green LED:** connection active / cable or USB device connected.
2		This button appears wherever there are settings that can be changed. It saves the current configuration temporarily, i.e. if the router is restarted, any changes to settings will be lost. To save settings permanently, click button no.5
3		If you saved your settings temporarily (see no.2), you can undo the changes by clicking on this button.
5		This permanently stores and applies all saved changes.
6		This is a check box. Clicking on a box enables/disables the option associated with it.
7		If input is required in a field that looks like this, it must be entered manually.
8		Clicking on a checked box will present the available options as a drop-down field.
9		Clicking on this field allows you to change (edit) settings in the associated row.
10		To reverse changes made to the associated row, click on this button.
11		Use this to do a temporary save of the settings that you are currently working on. To save changes to the router permanently, click button no.5.
12		This inserts additional input rows The currently displayed row must contain values or data before you click on this button. If not, an error message will appear at the top of the open configuration page.
13		This deletes the input of the row that you are currently working on.
14		This enables you to change the order of rules.

8.3 System settings

Before configuring the *mbNET* industrial router for your particular application requirements, you need to implement some specific basic settings.
Proceed as follows:

- ❑ On the navigation bar at the top bar on the web interface home page, click **System** and **Settings**.
  This will display the system settings screen shown below.
  Now proceed as described on the pages that follow.

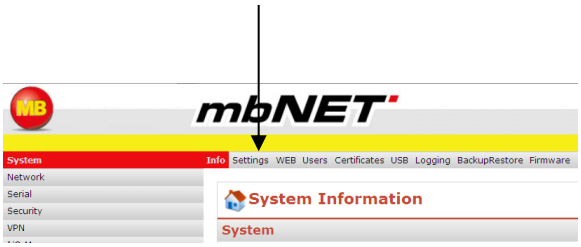


Figure 23

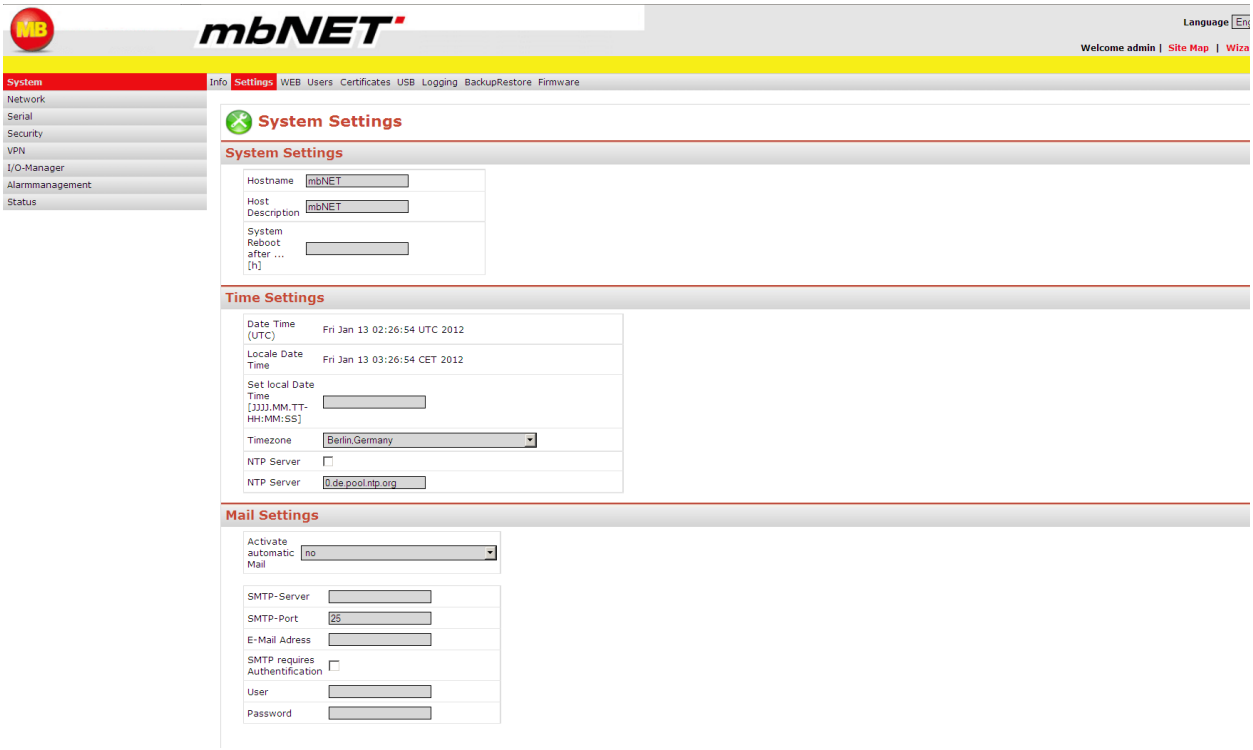


Figure 24

<table>
<tr><th>Label</th><th>Function</th></tr>
<tr><td>Hostname</td><td>Assign a name to the router.</td></tr>
<tr><td>Host Description</td><td>To identify the device within a network, provide a meaningful description here.</td></tr>
<tr><td>Date / Time (UTC)</td><td>Displays the current system time in Universal Time Coordinates (UTC).</td></tr>
<tr><td>Local Date / Time</td><td>Displays the time based on local time zone.</td></tr>
<tr><td>Set Local Date / Time</td><td>Enter the time here in case there is no NTP server installed, or in case it is unavailable. Example: 2007.10.30-13:33:00
<table>
<tr><th>Format</th><th>Meaning</th></tr>
<tr><td>YYYY</td><td>Year e.g. 2007</td></tr>
<tr><td>MM</td><td>Month e.g. 10</td></tr>
<tr><td>DD</td><td>Day e.g. 30</td></tr>
<tr><td>HH</td><td>Hour e.g. 13</td></tr>
<tr><td>MM</td><td>Minute e.g. 34</td></tr>
<tr><td>SS</td><td>Seconds e.g. 48</td></tr>
</table></td></tr>
<tr><td>Timezone</td><td>Click on the drop-down field and select the time zone where you are. The preset time zone is: Berlin, Germany</td></tr>
<tr><td>NTP server</td><td>Checking this box gives control of the router's time zone to another computer (which must be entered in the next input field) and displays the current system time.
The time is updated by NTP every two hours.
Registered time server: 134.176.25</td></tr>
<tr><td> </td><td>The mbNET has an RTC (buffered clock). The set time will buffer for up to 7 days without a power supply</td></tr>
<tr><td>NTP server</td><td>Specifies a time server for updating system time. A time server IP address may be entered instead of a name. If a name is entered, there must be a DNS server entered in the network settings,
or an existing Internet connection. The NTP server simply needs to be available.</td></tr>
<tr><td>Mail settings</td><td>Selecting "yes" in "Activate automatic mail" means that the router will use MB Connect Line's mail server and fixed parameters.</td></tr>
<tr><td>SMTP server</td><td>The SMTP server is needed for the router to send emails.</td></tr>
<tr><td>SMTP port</td><td>The port over which emails will be sent should be entered here. Usually this is port 25.</td></tr>
<tr><td>E-mail address</td><td>Enter the appropriate sender address for emails from the router here.</td></tr>
<tr><td>SMTP requires authentication</td><td>The box should be checked or unchecked depending on ISP. Ask your ISP for the correct setting.</td></tr>
<tr><td>User
Password</td><td>A user name and password are required for SMTP server authentication, i.e. if the router wants to send an email to the SMTP, it must first authenticate itself if necessary.</td></tr>
</table>

8.4 Security Settings

To access the industrial router's web interface from outside the network, Port 80 of the router's integrated firewall must be configured to receive incoming requests.

- ❑ To do this, select **Security – Settings – WAN>LAN**.
- ❑ Click on the check box to check it.

Figure 25

- ❑ From the drop-down field, select **Accept** (Fig. 27)

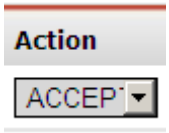


Figure 26

- ❑ From the **Protocol** drop-down field, select **tcp**.
- ❑ In Destination Port, enter **80**.
- ❑ Then save your settings by clicking on **Save Changes.**

Figure 27

Figure 28

- ❑ To save permanently, click **Apply Changes.**

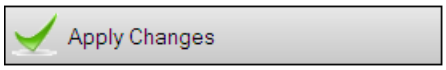


Figure 29

8.4.1 Save Settings

When you have completed the system settings described above, save these temporarily by clicking **Save Changes.**

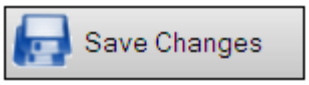


Figure 30

If you want to undo your changes and return to the original settings, click **Clear Changes.**

Figure 31

To save the settings permanently on the *mbNET* industrial router, click **Apply Changes**.

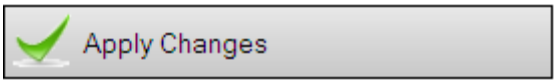


Figure 32

If any entries are missing or incorrect, the relevant error messages will appear at the top of the configuration page. Re-check your settings as appropriate.

Please note:
to ensure that your settings are permanently saved, you must follow the instructions above. Otherwise, you will lose your settings if the router is switched off or restarted.

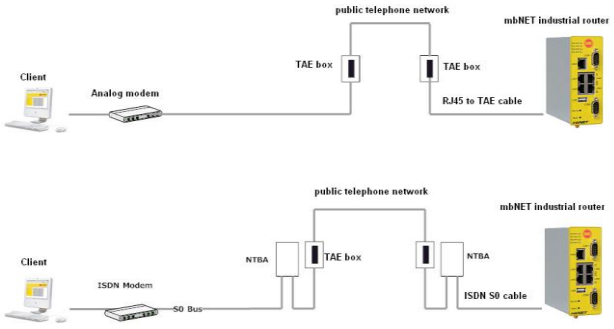
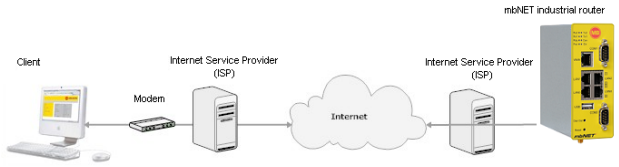
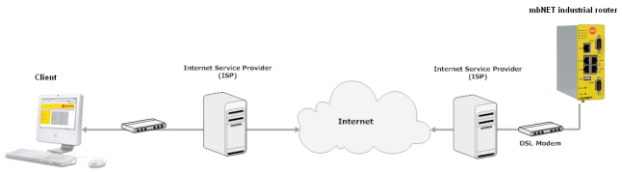
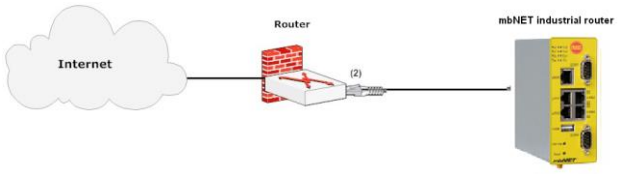
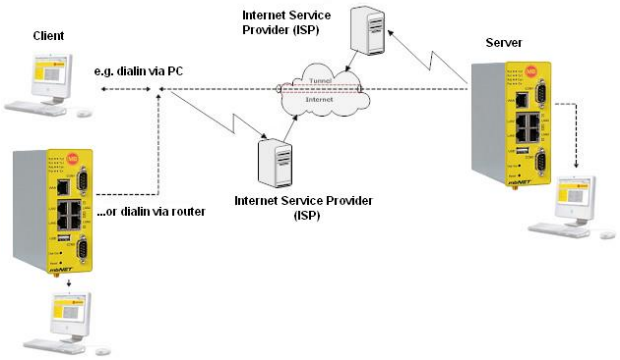
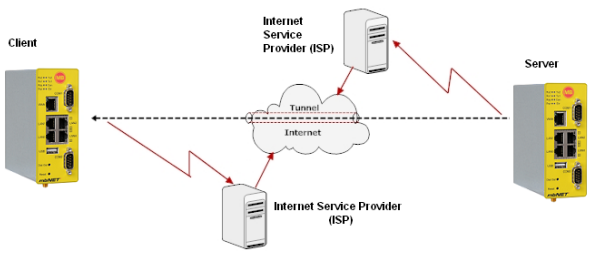
9. Connection Scenarios

9.1 General

Now that you have completed basic configuration of the router (see previous pages), it needs to be connected via the appropriate connection type, and configured using the web interface.

A description of some basic connection scenarios follows.

Choose the connection scenario that best applies to you and follow the instructions in the relevant section.

Configuring the mbNET industrial router's integrated modem for connection with a client PC via the public telephone network (PPP dial-up, dial-up networking) **see section 9.2**	
Configuring the mbNET industrial router's integrated modem for connection with a client PC via the Internet **see section 9.3**	
Configuring the mbNET router for connection with a client PC via DSL Internet access, using a DSL modem **see section 9.4**	
Configuring the mbNET industrial router for connection to the Internet using another router **see section 9.5**	
Configuring the mbNET industrial router for VPN connection with a client (client – router) **see section 9.6**	
Configuring an mbNET industrial router for VPN connection to another mbNET router (router – router) **see section 9.7**	

9.2 Configuring the industrial router for connection over the telephone network

The following diagram shows how to connect the industrial router to a client over the **public telephone network.**
Using this type of connection, the industrial router can be accessed over the telephone network via its serial interfaces (see **Serial Interfaces**) and LAN interface.
In the following example, the client is a PC with a modem connection.

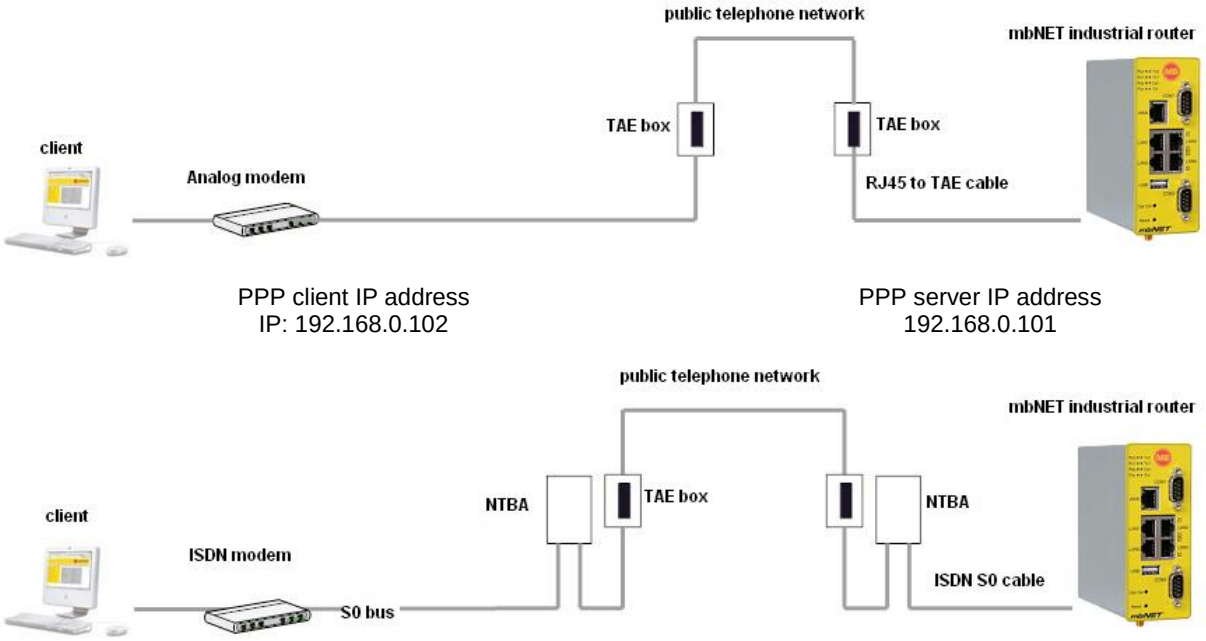


Figure 33

9.2.1 Connecting and configuring the router

Before you being:
The router should be connected to a suitable power source, and the **Power** and **Ready** LEDs should be solid green.

9.2.1.1 Connecting the router

Analog connection
(applies to device models MDH xx0)

- ❑ Connect TAE adapter to analog cable.
- ❑ Plug one end of the supplied cable into the RJ12 jack (**1**) on the bottom of the router, and the other end into the TAE jack (**2**).

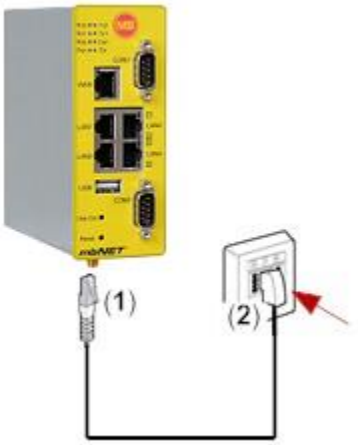


Figure 34

ISDN connection
(applies to device models MDH xx2)

- ❑ With an existing **ISDN connection,** plug one end of the ISDN cable into the jack (**1**) on the bottom of the router and the other end into the (**2**) **NTBA.**

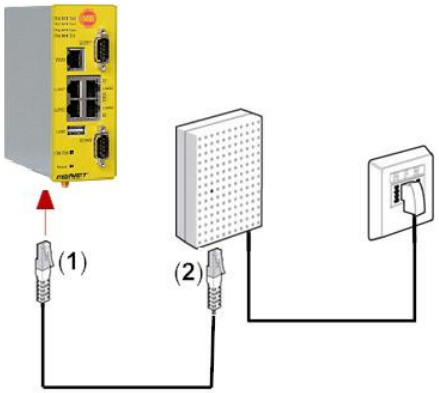


Figure 35

GSM connection:
(applies to device models MDH xx3 and MDH xx4)

- ❑ With an existing **GSM connection,** plug the end of the GSM antenna cable into the jack on the bottom of the router.

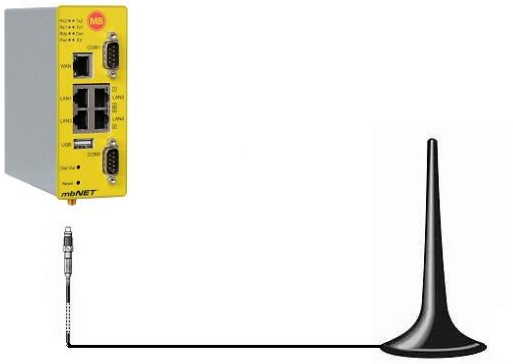


Figure 36

9.2.1.2 Configuring the router using the web interface

- ❑ On the web interface home page, click on **Network** – **Modem**.

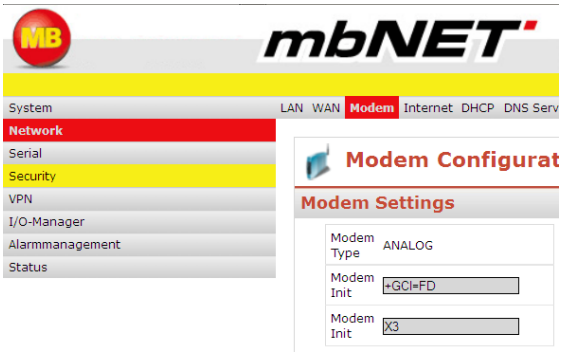


Figure 37

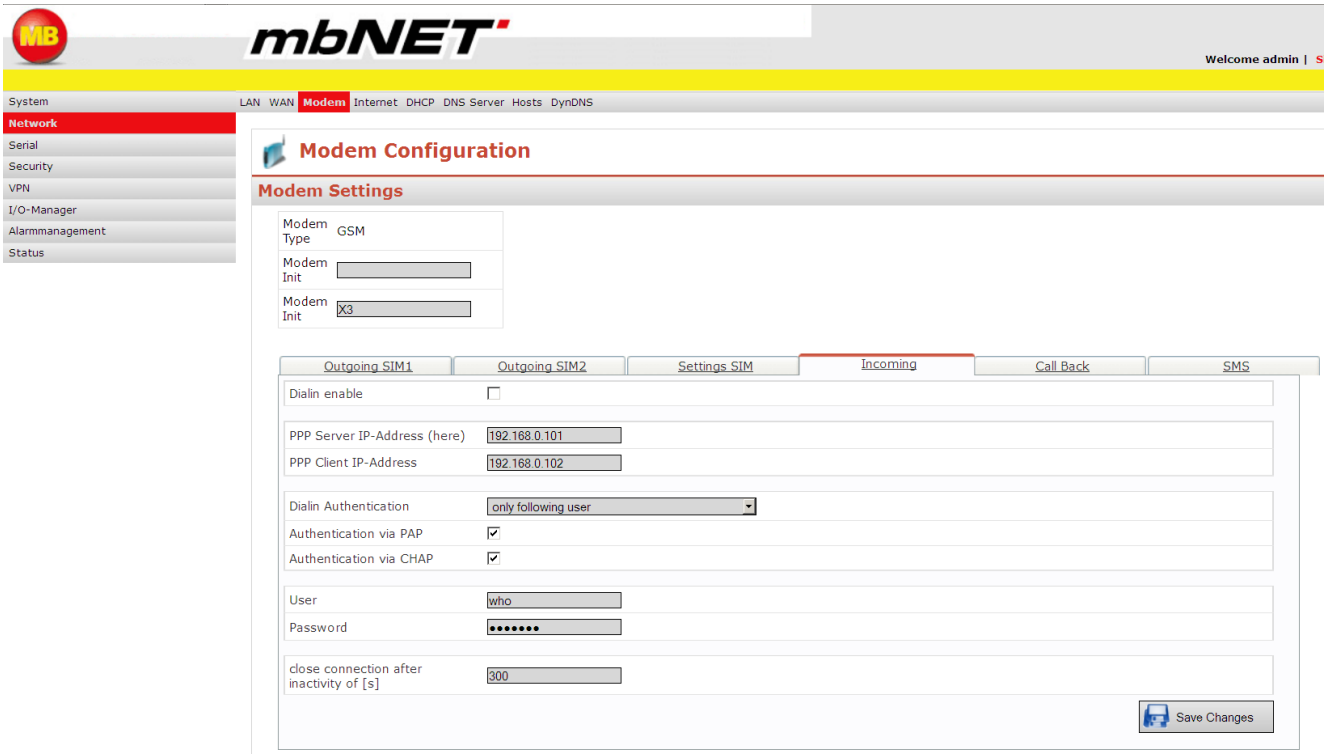


Figure 38

For more detailed information on this, please see section *Network – Modem*

Label	Description
Modem Init	**ANALOG:** if using an analog device, enter the command **+GCI=country code** (for country codes, see **Country codes for analog devices**) here, and in the second row, the command **X3** (do not wait for dial tone). **ISDN:** if using an ISDN device, you need to enter your MSN (multiple subscriber number) with the command **AT#Z=n** (n= MSN number) If you enter "n" as "*", every call will be accepted. **GSM:** if using a GSM device, you can either keep the preset **X3** command, or use the **+GCI=country code** command.
SIM PIN (GSM only)	If required, you can enter the SIM card PIN here. However, the device will also work without SIM card PIN protection
Provider (GSM only)	You can select your mobile broadband provider here. If it does not appear, select "Other"
Provider name (GSM only)	If your provider was not shown, you can also manually enter the APN (Access Point Name) here. You can obtain details of the APN from your mobile broadband provider or from our website at http://www.mbconnectline.de/gsm/grps/mobilfunk.html
Incoming	
Dial-in enable	Click on the check box to check it and enable a client computer to connect to the *mbNET* via a dial-up connection.
PPP Server IP-Address (here)	Enter the IP-address of the PPP server. In this case: 192.168.4.100 This sets this address as the *mbNET* address for client computers dialing in
PPP Client IP-Address	Enter the IP-address that you want the client to receive. In this case: 192.168.4.101

Dial-in Authentication	From the drop-down field, select **only following user** (as shown here in the example),or **every User with dialin rights** This determines whether any user registered under System – User, or only one specific user, can dial in to the *mbNET*.
Authentication via PAP	Authentication protocol that transfers your login credentials (**P**assword**A**uthen-tication**P**rotocol). However, we recommend using the more secure CHAP vari-ant alongside this, as PAP sends your credentials unencrypted.
Authentication via CHAP	Authentication protocol that transfers your login credentials securely (**CH**al-lenge**HA**ndshake**P**rotocol)

- ❑ Now save your changes by clicking **Save Changes.**

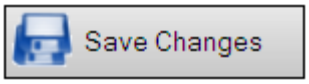


Figure 39

- ❑ Now click on **Network** – **Internet** and enter the following settings.

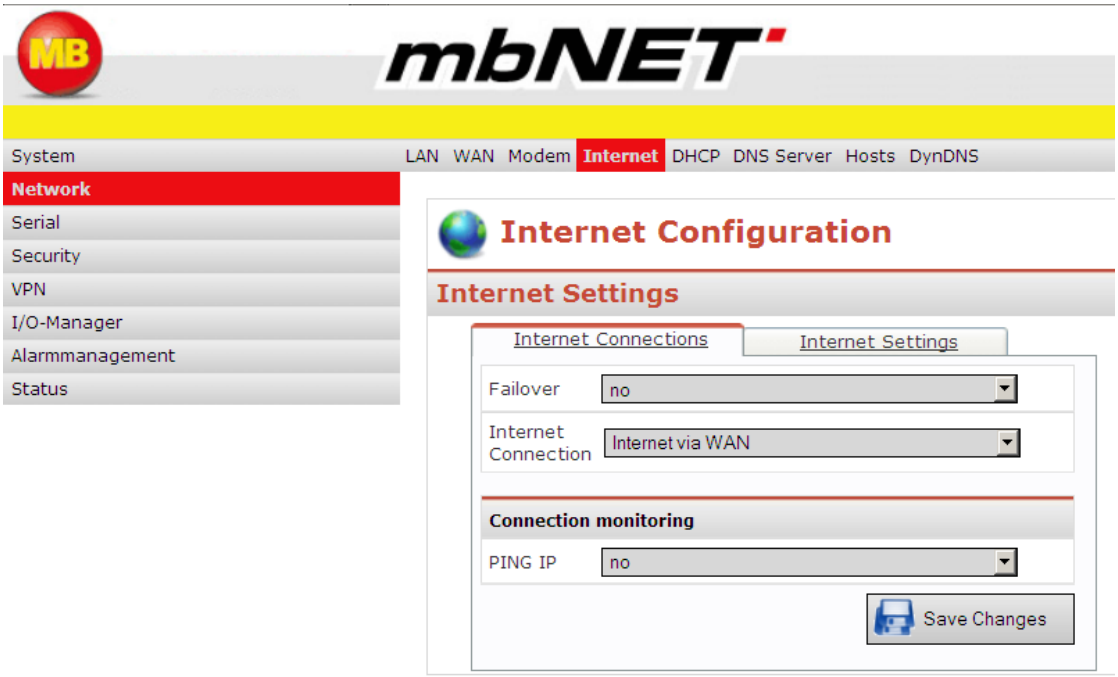


Figure 40

For a detailed description of the Network – Internet settings, please see section *Network – Internet*

Label	Description
Internet connection	Select either **Internet via modem** or **Internet via WAN.**

Configuring the router – client connection over the telephone network (continued)

- Save your changes by clicking **Save Changes.**

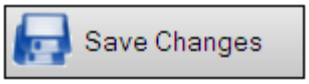


Figure 41

- Click on **System** – **User** and add a user with dial-in rights. For further notes on adding users and assigning specific rights, please see section ***Adding users***

- Finally, to save your changes permanently to the industrial router, click **Apply Changes.**

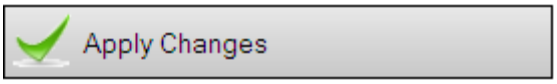


Figure 42

For devices to be able to communicate with the LAN interface, they must be configured using the *mbNET* LAN interface IP address as the device gateway.
Communication is not via PPP addresses, but via the *mbNET* LAN interface IP address and the IP addresses of connected devices.

9.2.2 Configuring a client (PC) to access the router

You can connect directly to the router, and to a remote network, using a telephone line. Router access must first be correctly configured as described above. Then you need to set up a suitable dial-up connection on the computer, as follows.

- ❑ Click on START and then Control Panel.
- ❑ Click on NETWORK CONNECTIONS and then NEW CONNECTION WIZARD. This launches the connection wizard which will make all the necessary settings.

  The welcome screen of the connection wizard will appear. Click **NEXT.**

New Connection Wizard
Welcome to the New Connection Wizard
This wizard helps you:
• Connect to the Internet.
• Connect to a private network, such as your workplace network.
• Set up a home or small office network.
To continue, click Next.
< Back
Next >
Cancel

Figure 43

- ❑ In Network Connection Type, choose the second option, **Connect to the network at my workplace** and then click **NEXT.**

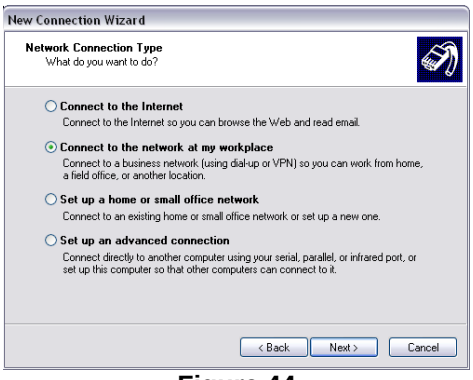

New Connection Wizard
Network Connection Type
What do you want to do?
Connect to the Internet
Connect to the Internet so you can browse the Web and read email.
Connect to the network at my workplace
Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.
Set up a home or small office network
Connect to an existing home or small office network or set up a new one.
Set up an advanced connection
Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it.
< Back
Next >
Cancel

Figure 44

- ❑ Choose **Dial-up connection** and the modem that you wish to use to set up a connection with the industrial router.

New Connection Wizard
Network Connection
How do you want to connect to the network at your workplace?
Create the following connection:
Dial-up connection
Connect using a modem and a regular phone line or an Integrated Services Digital Network (ISDN) phone line.
Virtual Private Network connection
Connect to the network using a virtual private network (VPN) connection over the Internet.
< Back
Next >
Cancel

Figure 45

Configuring the router – client connection over the telephone network (continued)

- ❑ Now you need to give your connection a name,
  then click **NEXT.**

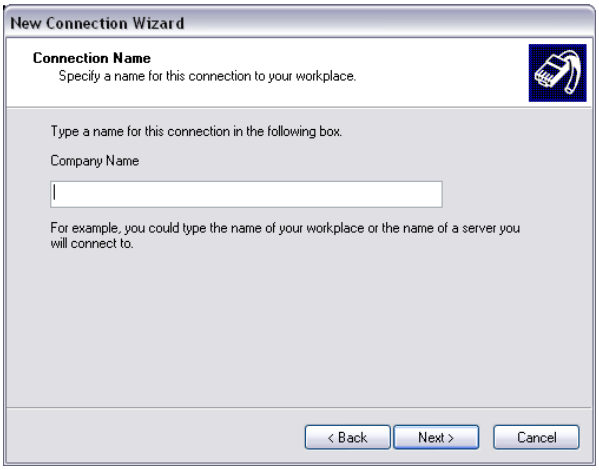

New Connection Wizard
Connection Name
Specify a name for this connection to your workplace.
Type a name for this connection in the following box.
Company Name
For example, you could type the name of your workplace or the name of a server you will connect to.
< Back
Next >
Cancel

Figure 46

- ❑ Enter the telephone number of your remote station (the number that accesses the industrial router)

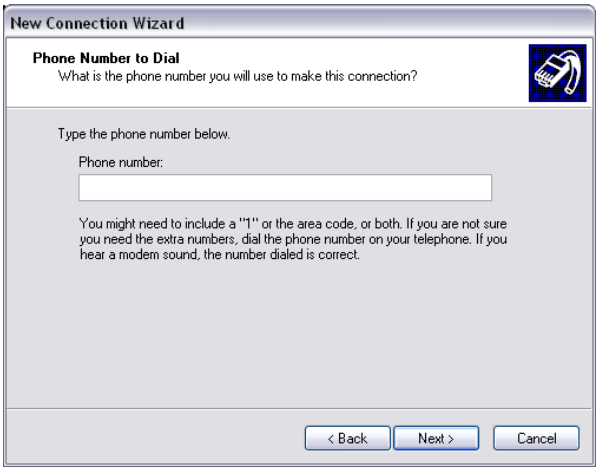

New Connection Wizard
Phone Number to Dial
What is the phone number you will use to make this connection?
Type the phone number below.
Phone number:
You might need to include a "1" or the area code, or both. If you are not sure you need the extra numbers, dial the phone number on your telephone. If you hear a modem sound, the number dialed is correct.
< Back
Next >
Cancel

Figure 47

- ❑ Click **Finish**.

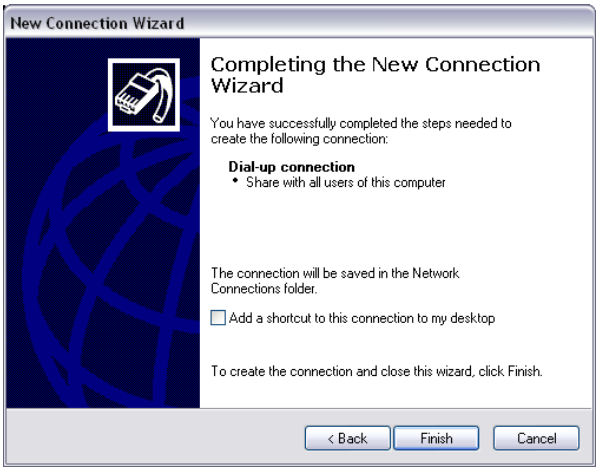

New Connection Wizard
Completing the New Connection Wizard
You have successfully completed the steps needed to create the following connection:
Dial-up connection
• Share with all users of this computer
The connection will be saved in the Network Connections folder.
Add a shortcut to this connection to my desktop
To create the connection and close this wizard, click Finish.
< Back
Finish
Cancel

Figure 48

9.2.3 Establishing a connection between the client PC and the industrial router

- ❑ Double-click on the connection that you created using the instructions in the previous section.
- ❑ In this window, enter the **user name** and **password** that you created previously when configuring the modem. If you selected the option "every User with dialin rights", you can enter the user name and password of any user who has dial-in rights.

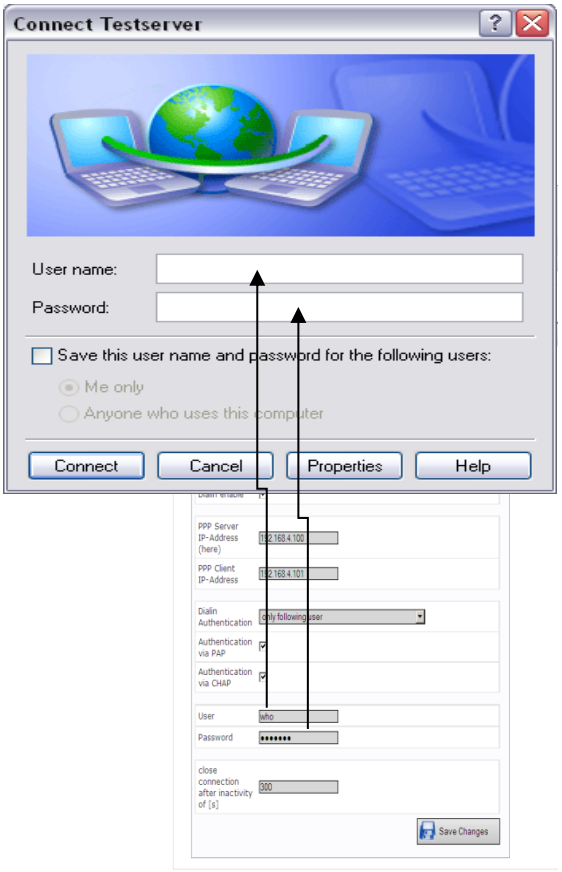


Figure 49

The default settings for **Authentication via CHAP** and **Authentication via PAP** must be the same as those on the router, otherwise no connection can be established.

- ❑ Click **Connect.**

- ✓ **You have established a connection to the router.**

9.2.4 Displaying and verifying connection status

On a computer connected to the router's LAN interface, clicking on **Status** – **Modem** shows whether a user has dialed in to the router, and where there is an established connection, who has dialed in.

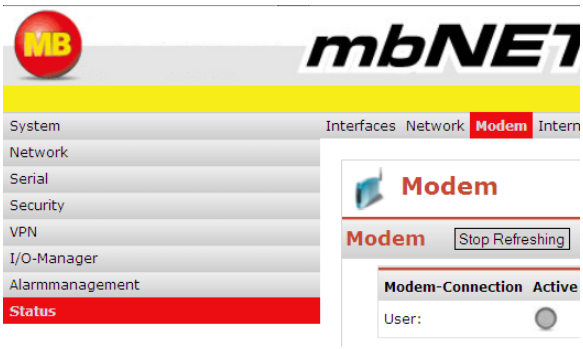


Figure 50

9.3 Configuring the industrial router for connection via the Internet

The following diagram shows how to connect the industrial router to a client computer via the Internet. The client is a computer with a modem connection.

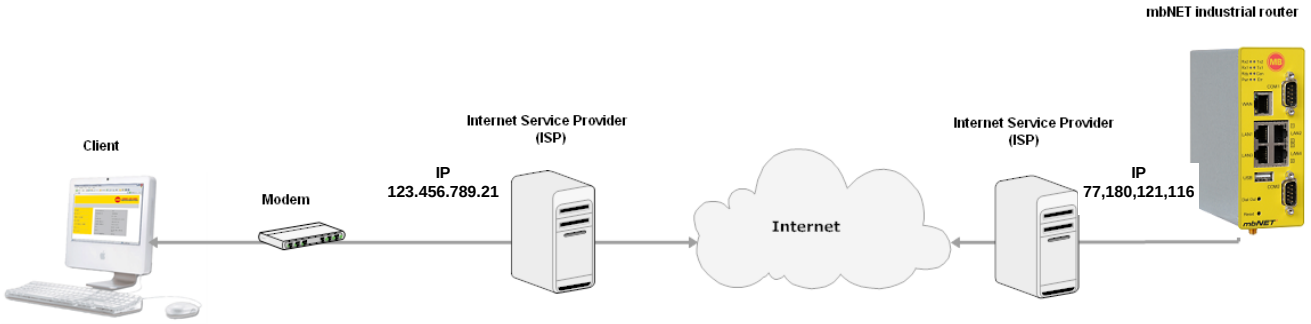


Figure 51

9.3.1 Connecting and configuring the router

Before you begin:
The router should be connected to a suitable power source and the **Power** and **Ready** LEDs should be solid green.

9.3.1.1 Connecting the router

Analog connection only (applies to device models MDH xx0)

- ❑ Connect TAE adapter to analog cable.
- ❑ Plug one end of the supplied cable into the RJ12 jack (**1**) on the bottom of the router, and the other end into the TAE jack (**2**).

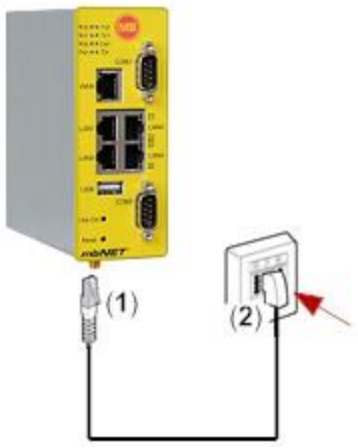


Figure 52

ISDN connection only (applies to device models MDH0x2)

- ❑ Plug one end of the supplied cable into the jack (**1**), and the other end into (**2**) the **NTBA.**

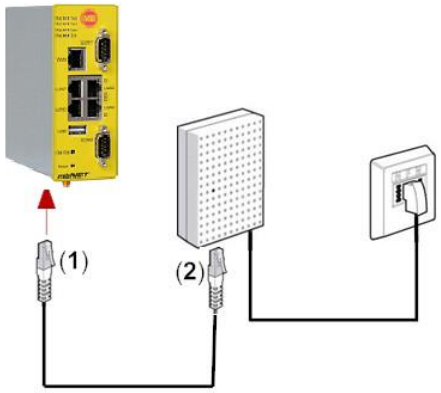


Figure 53

GSM connection only (applies to device models MDHxx3 and xx4)

- ❑ Plug one end of the supplied antenna cable into the jack.

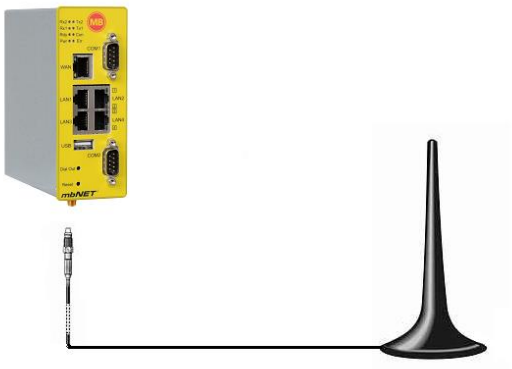


Figure 54

9.3.1.2 Configuring the router using the web interface

- ❑ You can configure your connections quickly and easily using the connection wizard. To do this, click on the Wizards link at the top right of your browser. If you have disabled the autolaunch function for wizards, click on the Start button for the Internet connection wizard.

- ❑ Here, choose the Modem option and click "Next"

- ❑ If your ISP is already stored on the mbNET, click on "use a Provider from list". Alternatively you can enter your own by choosing "enter APN manually" and entering your ISP details.

- ❑ If the mbNET is to be used behind a telephone system, activate the box next to "Use the following dialout number" and then click "Next"

- ❑ You can also choose whether the mbNET should send you an email with the current public address, use a dynamic DNS service, or be accessible over the Internet via MB Connect Line's DynDNS.

Figure 55:

To configure manually, proceed as follows:

From the home page, click **Network** and **Modem** and then on the Outgoing tab.

- ❑ The following screen (see next page) will be displayed. Follow the instructions on the subsequent pages.

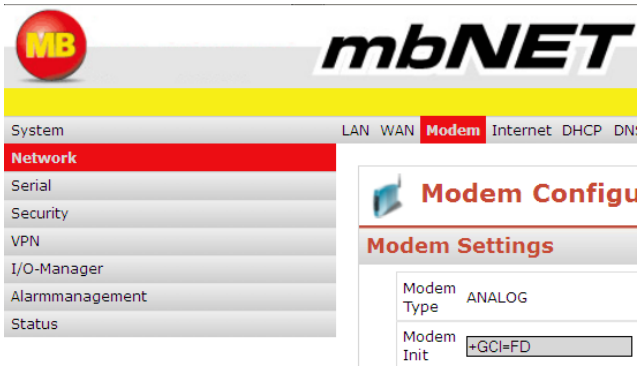


Figure 56

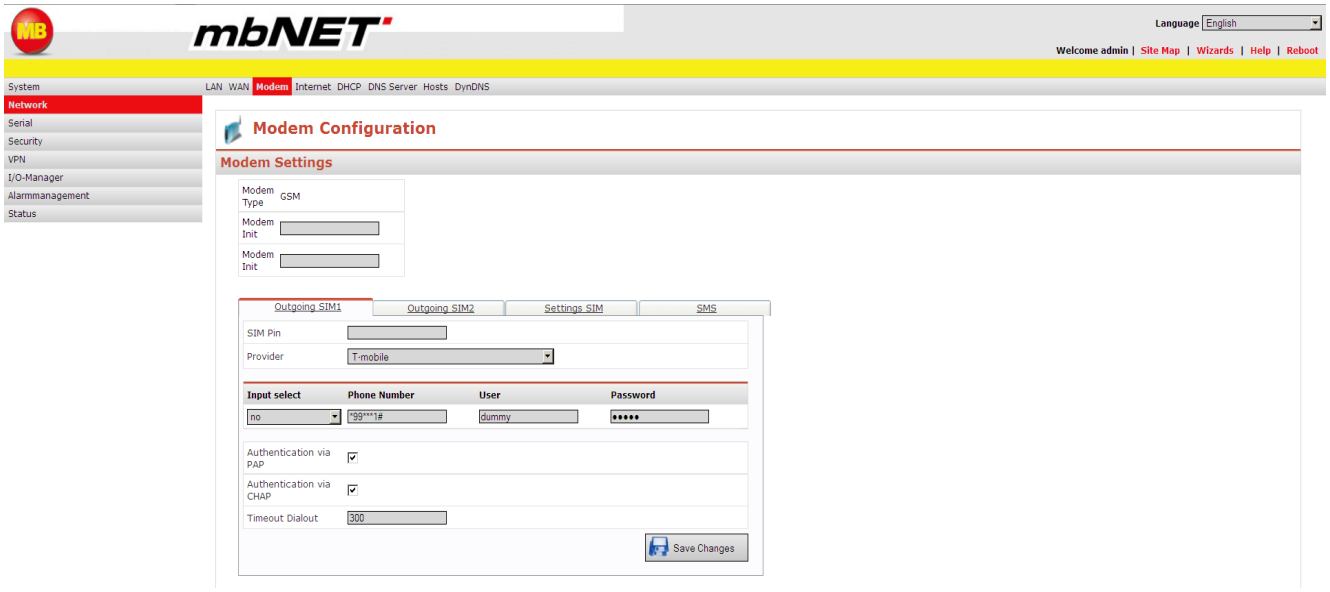


Figure 57

For a detailed description of the Network – Modem settings, please see section *Network – Modem*

Label	Description
Modem Init	**ANALOG:** If using an analog device, enter the command **+GCI=country code** (for country codes, see **Country codes for analog devices**) here, and in the second row, the command **X3** (do not wait for dial tone). **ISDN:** If using an ISDN device, you need to enter your MSN number with the command **AT#Z=n** (n= MSN number) If you enter "n" as "*", every call will be accepted. **GSM:** if using a GSM device, you must use the preset X3 command. The **+GCI=country code** may not be used.
SIM PIN (GSM only)	If required, you can enter the SIM card PIN here.
Provider (GSM only)	You can select your provider here. If your provider is not shown, you can enter the APN (Access Point Name) yourself. You can obtain information on the APN from our website at http://www.mbconnectline.de/gsm/grps/mobilfunk.html or from your mobile broadband provider.
Provider name	If you do not see your provider listed, you can enter your APN manually. Ask your provider what details to enter for the APN, or visit our website at http://www.mbconnectline.de/gsm/grps/mobilfunk.html
Phone number	Enter the telephone number of the relevant provider. For example, the dial-up number for an analog data call: 019193384 **See comment below table.** For **GSM** Modems the dial-up number always uses the format ***99***1#**
User	Enter user name (refer to your mobile broadband provider's network details) In example shown: any For GSM modems you can obtain the necessary information at e.g.

	http://www.mbconnectline.de/gsm/grps/mobilfunk.html (In most cases, any user name can be used).
Password	Enter password (from provider details). In example shown: any For GSM modems you can obtain the necessary information at e.g. http://www.mbconnectline.de/gsm/grps/mobilfunk.html (In most cases, any password can be used).
Authentication via PAP	Use the default setting for the authentication protocol. This is set by default when a dial-up connection is set up.
Authentication via CHAP	Use the default setting for the authentication protocol. This is set e.g. when a dial-up connection is set up.
Timeout dialout in [s]	Enter a time of 300 (=5 minutes in the example shown here), after which dialing attempts will stop.

- ❑ Save your changes by clicking **Save Changes.**

Figure 58

Please note:

Dial-up providers change their tariffs frequently. MB Connect Line cannot be held responsible for possible price changes.

Configuring for connection over the Internet (continued)

- ❑ From the web interface home page, click **Network** and **Internet**

  The following screen will be displayed.
  Follow the instructions below.

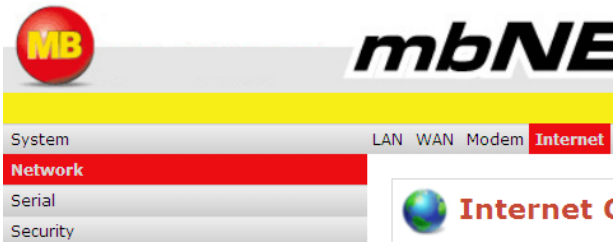


Figure 59

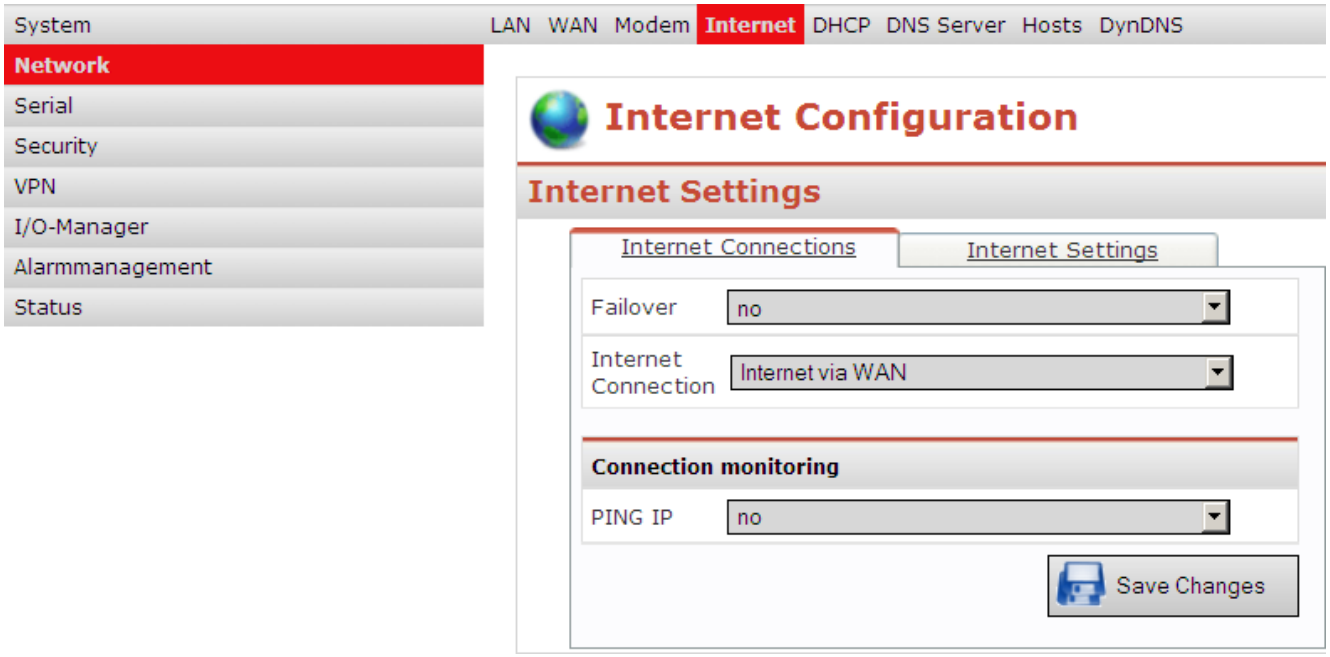


Figure 60

For a detailed description, see Network – Internet

Item	Label	Description
1	**Internet connections**	From the drop-down field, select the setting **Internet via modem**
2	**Connection Mode**	Select **Keep connection**
3	**Lock connection by**	Using the drop-down field you can decide whether the Internet connection should be closed when one of the inputs receives a signal (internally-generated, between 10 and 30V).
4	**Send IP address via email**	Enable this setting. Select whether the IP address should be sent to the email address listed.
5	**Email**	Enter the email address to which the IP address is to be sent here.

- ❑ Save your changes by clicking **Save Changes.**
- ❑ Finally, to save your changes permanently to the router, click **Apply Changes.**

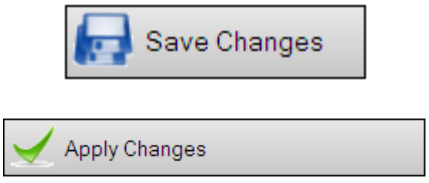


Figure 61

9.3.2 Router Internet dial-in

In the screen shown above, the router is configured to establish an Internet connection as soon as it is restarted.

For other methods of Internet dial-in, please see section **Network – Internet**

- **Transmit IP address**
  For the client to be able to access the router, it must know the router's IP address**.** Under the configuration settings made previously, the IP address is sent to the email address that was provided. This allows you to access the router via the IP address.

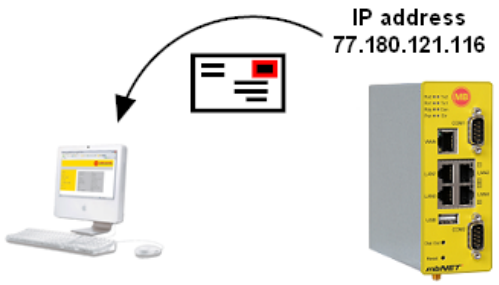


Figure 62

As the router IP address changes each time it dials in to the Internet, there is an alternative, which is to use our **DynDNS service**. For information on setting up and using the MB Connect Line DynDNS service, please see section ***Network – DynDNS***

9.3.3 Displaying the Internet connection

Provided that you can access the router, you can see information on the status of the Internet connection by clicking
Status – **Internet**.

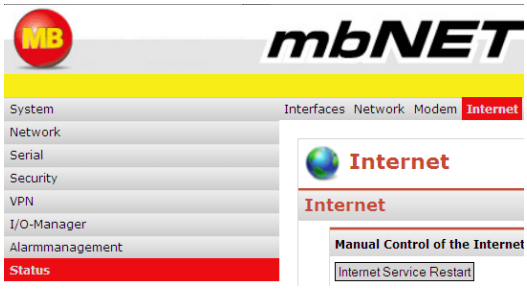


Figure 63

For information on status messages, please see section *Status Messages*

9.4 Configuring the industrial router for connection to the Internet using a DSL modem

The diagram below shows how to connect the *mbNET* industrial router to a client PC over the Internet, using a DSL modem.
The client needs to use an existing Internet connection, or to set one up.

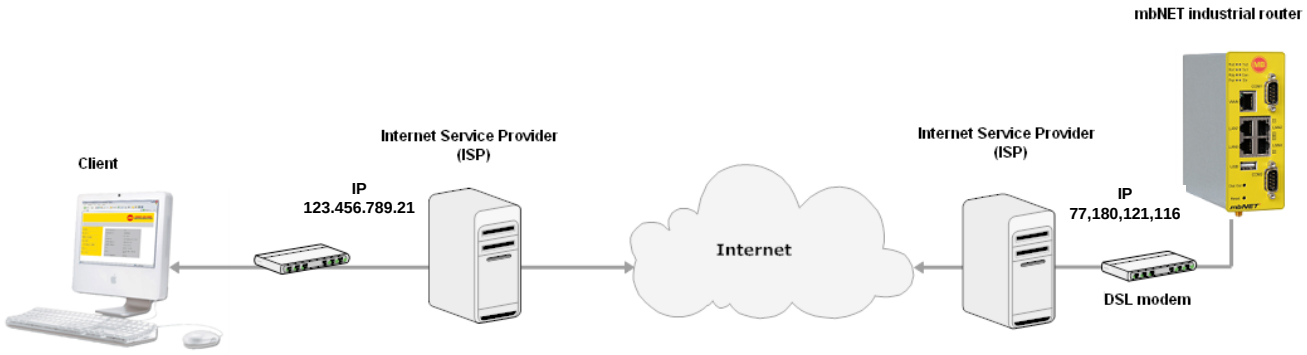


Figure 64

Configuring for connection over the Internet (continued)

9.4.1 Connecting and configuring the router

Before you begin:
The router must already be connected to a suitable power source and the **Power** and **Ready** LEDs must both be solid green.

9.4.1.1 Connecting the router

- ❑ Connect the router to the DSL modem as shown in the diagram on the right.
- ❑ To do this, plug one end of the straight-through Ethernet cable into the LAN connector (1) of the DSL modem and the other end (2) into the WAN connector on the router.

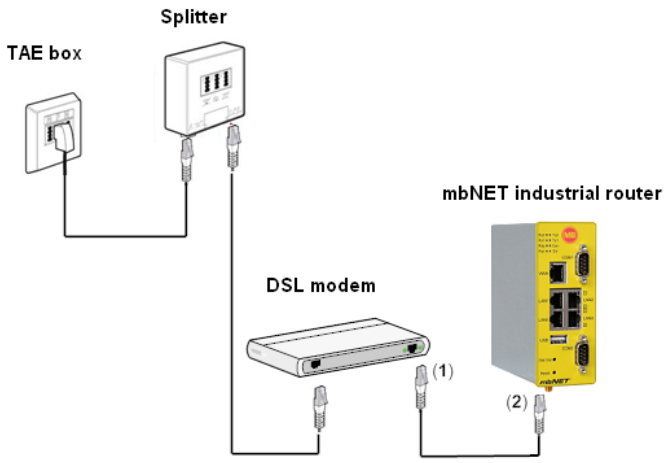


Figure 65

9.4.1.2 Configuring the router using the web interface

- **The connection wizard** helps you to configure your connections quickly and easily. To access the wizard, click on the Wizards link at the top right of your browser. If you have disabled the autolaunch function for wizards, click on the Start button for the Internet connection wizard.

- Now select the option for External DSL modem.

- Enter your Internet login details. You can obtain these from your Internet Service Provider.

- You can also choose whether the mbNET should send you an email, use a dynamic DNS service, or be accessible over the Internet via MB Connect Line's DynDNS.

- Confirm and save your entries. Finally, the mbNET must be restarted to fully implement the settings.

- From the home page of the configuration interface, click **Network – WAN** and then the Outgoing tab. This will display the screen shown below. Follow the instructions below.

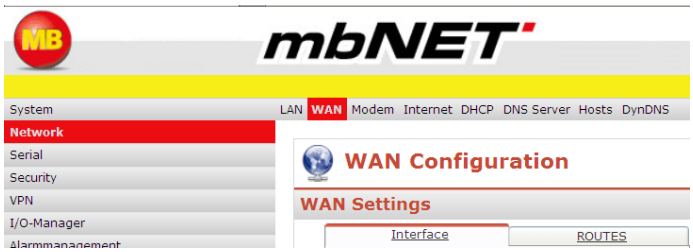


Figure 66

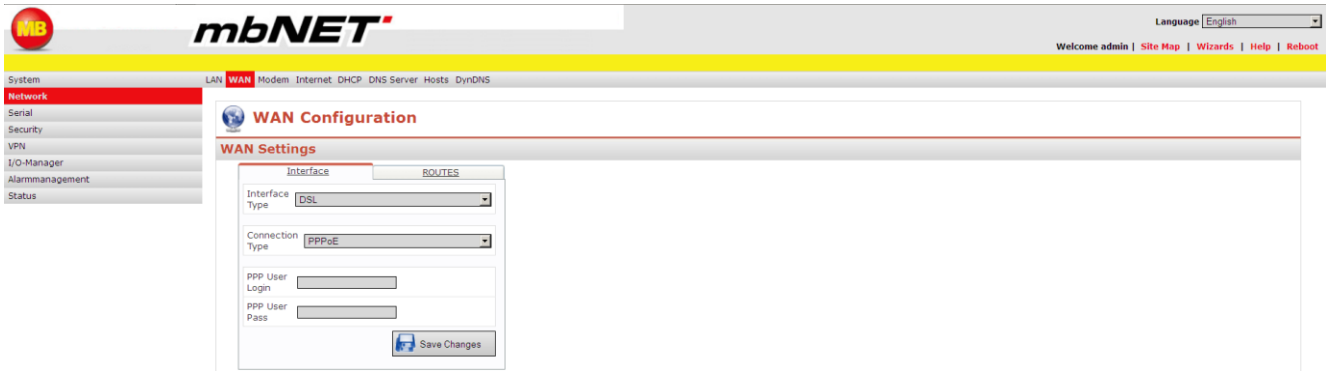


Figure 67

For a detailed description of Network – WAN settings, please see section *Network – WAN*

Label	Description
Interface Type	Here, select **DSL**.
Connection Type	If you are in Germany, select **PPPoE** (most commonly used protocol in Germany). PPTP is most common in Austria.
PPP User Login	Enter your Internet access user name. Use the name provided by your ISP.
PPP User Pass	Enter your Internet access password. Use the password provided by your ISP.

❑ Save your changes by clicking **Save Changes.**

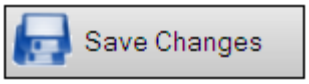


Figure 68

Configuring for connection over the Internet (continued)

- From the web interface home page, click **Network** – **Internet**
- The following screen will be displayed. Proceed as follows:

Figure 69

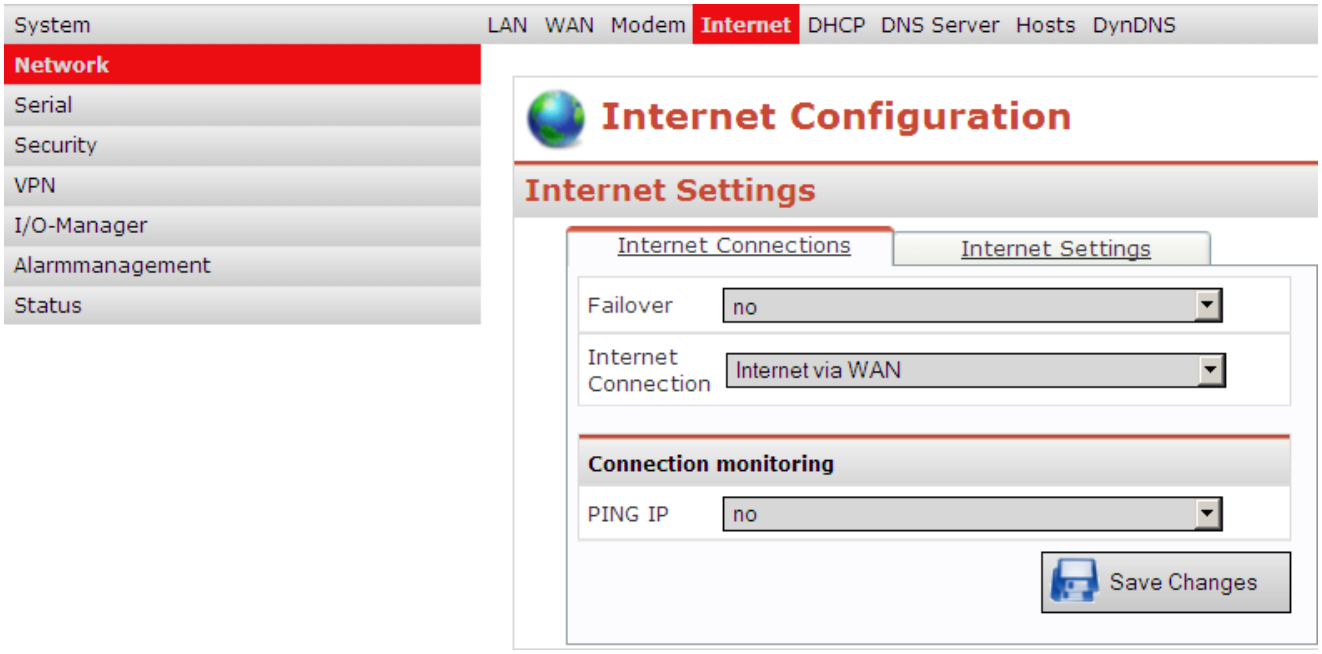


Figure 70

For a detailed description of the Network – Internet settings, please see section *Network – Internet*

Label	Description
Internet connections	Here, select to connect over **Internet via WAN**.
Connection Mode	Select **Connect immediately.** The connection will be established whenever you restart the router.
Lock connection by	You can interrupt the Internet connection by means of a signal to one of the digital inputs.
Send IP address via email	Check the box by clicking on it, to have the router's IP address sent to the email address that you will enter below.
Email	When an Internet connection has been established, an email message will be sent to the email address entered here.

- ❑ Save your changes by clicking **Save Changes.**

- ❑ Finally, to save your changes permanently to the router, click **Apply Changes.**

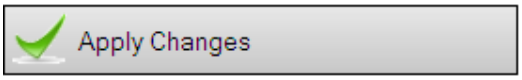


Figure 71

- ❑ To finish, ***restart the router***.

9.4.2 Establishing a connection between client PC and router

- ❑ Router Internet dial-in. Depending on the router settings (see Internet Configuration), you need to either restart the router, or push the Reset button.

For further Internet dial-in settings, please see section Network – Internet

- ❑ Client PC Internet dial-in. Dial the client PC into the Internet.

Figure 72

- ❑ Transmit IP address
  For the client to be able to access the router, it must know the router's IP address. The option to transmit the IP address is selected during router configuration. The IP address is identified by sending it to the email address specified during configuration.

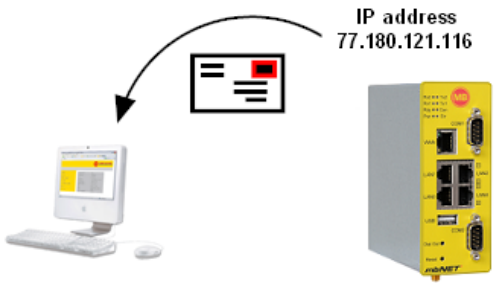


Figure 73

As the router IP address changes each time it dials up to the Internet, a helpful alternative is to use our **DynDNS service**.
For information on setting up and using the MB Connect Line DynDNS service, please see section Network – DynDNS

9.4.3 Displaying connection status

- ❑ Using a PC connected to the LAN interface, you can check for an active Internet connection by clicking on **Status** – **Internet**.

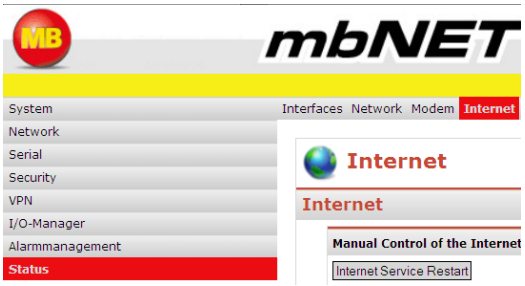


Figure 74

For further information on status messages, please see section Status Messages

9.5 Configuring the industrial router for connection to the Internet via an existing router

The diagram below shows how to link the industrial router up to a network which already has a router that is set up for connection to the Internet. The existing router must first be assigned the right settings. This operating mode is particularly useful if you need to set up a connection between the *mbNET* industrial router and a VPN gateway.

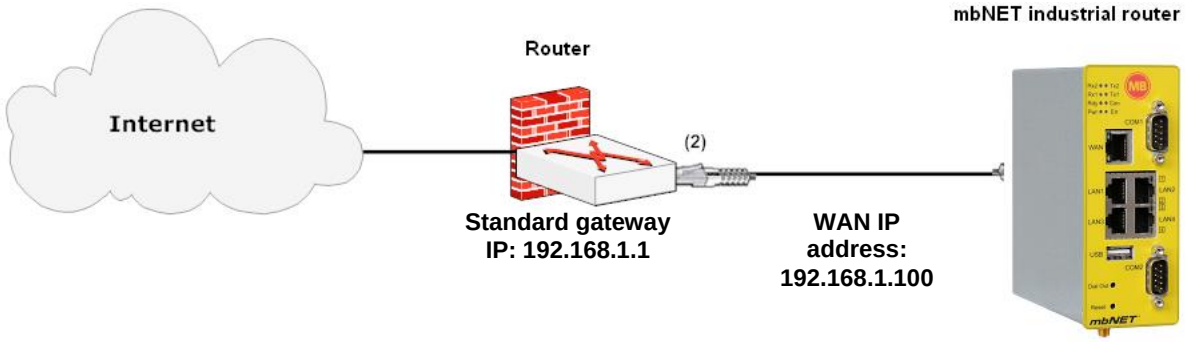


Figure 75

9.5.1 Connecting and configuring the router

9.5.1.1 Connecting the router

- ❑ Connect the router to the existing router as shown in the diagram on the right.
  - ❑ To do this, plug one end of the crossover cable (**1**) into the (**1**) **WAN** connector on the *mbNET* router, and the other end into the **LAN** connector (**2**) of the existing network router.

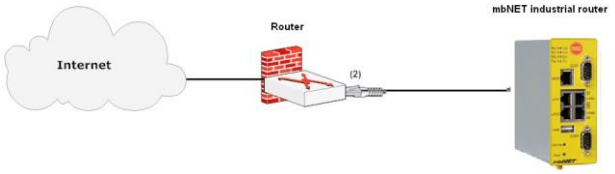


Figure 76

9.5.1.2 Configuring the router using the web interface

- **The connection wizard** helps you to configure your connections quickly and easily. To access the wizard, click on the Wizards link at the top right of your browser. If you have disabled the autolaunch function for wizards, click the Start button for the Internet connection wizard.

- Now select the option "External router (Firewall)".

- At this point you have a choice between automatic recognition of your network and interface details, or entering them manually.

- Read through the information and after clicking "Next", you can complete the wizard by clicking "Finish". A restart is required to complete the process.

- From the home page of the configuration interface, click **Network – WAN – Interface**. This will display the screen shown below.

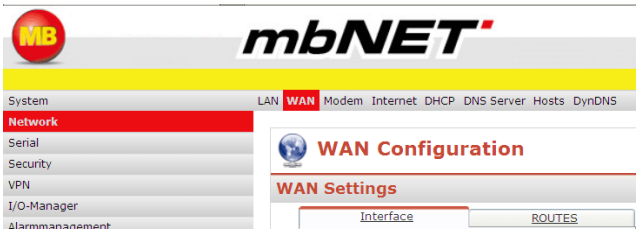


Figure 77

Configuring the router for connection to the Internet via an existing router

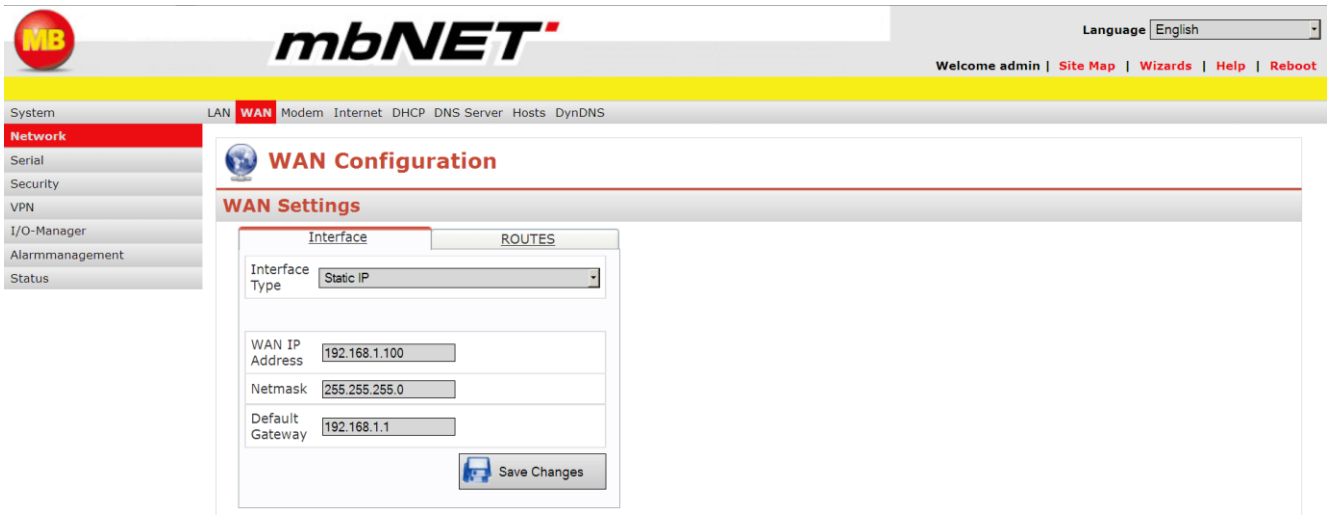


Figure 78

For a detailed description of the Network – WAN settings, please see section *Network – WAN*

Item	Label	Description
1	**Interface Type**	As in the example shown, select **Static IP.** This setting also requires a DNS server (see **Network – DNS server**).
2	**WAN IP Address**	Here, enter the IP address of the *mbNET* connected to the WAN port. In the example: 192.168.1.100
3	**Netmask**	Enter the subnet mask. In this case: 255.255.255.0
4	**Default Gateway**	Enter details of the gateway that connects you to the Internet, i.e. the IP address of the existing router. In this case: 192.168.1.1

- ❑ On the web interface home page, click on **Network** – **Internet**.
- ❑ The following screen will be displayed.
  Follow the instructions on the subsequent pages.

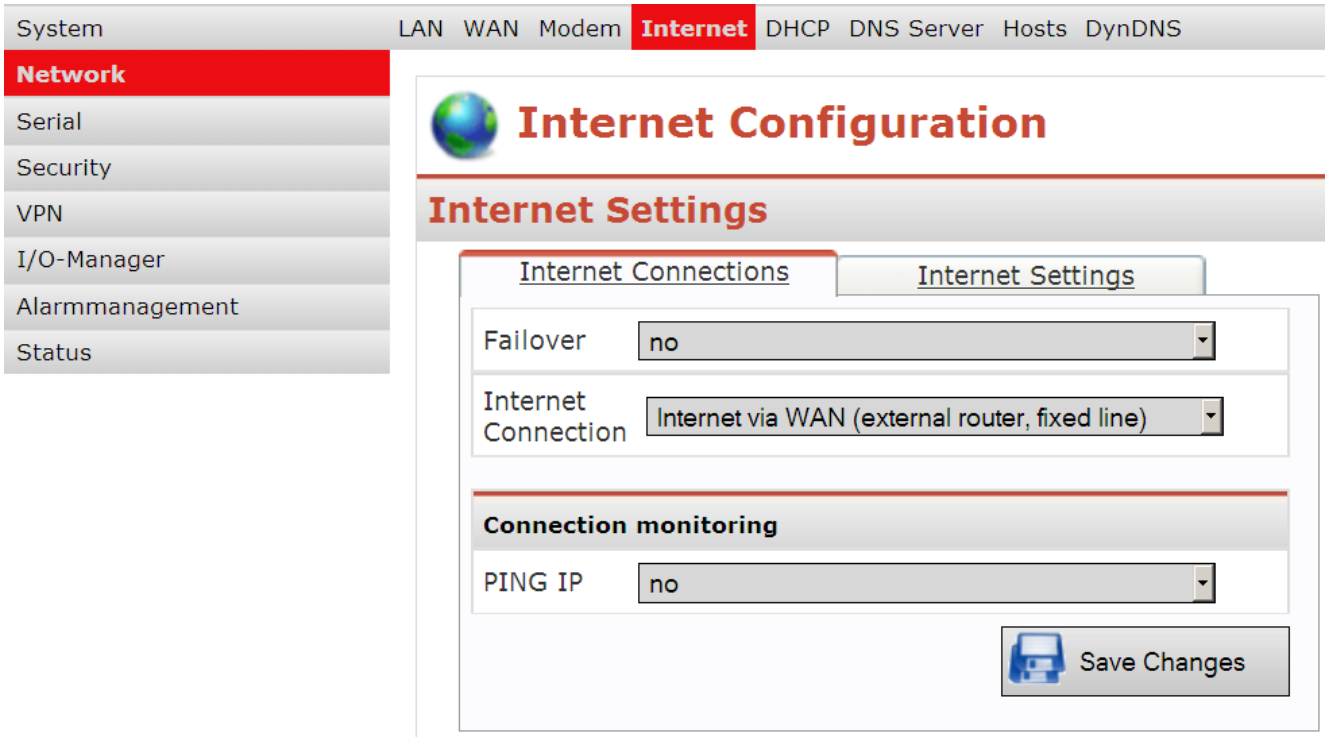


Figure 79

For a detailed description of the Network – Internet settings, please see section *Network – Internet*

Item	Label	Description
1	**Internet connection**	From the drop-down field, select **connect to Internet via WAN (external router, fixed line)**, so that the Internet connection will be made by the existing router.

This option means "no Internet connection" because the mbNET itself is not connecting to the Internet.

- ❑ Save your changes by clicking **Save Changes.**
- ❑ Finally, to save your changes permanently to the router, click **Apply Changes.**

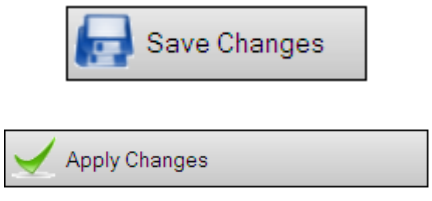


Figure 80

After applying the changes, please restart the router.

9.6 Configuring the industrial router for VPN connection to a client

Setting up a virtual network reduces the cost of a fixed connection between two or more LANs and ensures secure data transfer over the non-secure Internet. Using a tunneling protocol sets up a secure connection called a VPN tunnel.
In the connection scenarios described in 9.3 and 9.4, a client can only access the router's serial interfaces (for a description of serial interfaces, see **Serial Interfaces**). This does not allow for access to the LAN interface via the Internet. Using a VPN connection however, it is possible to reach or access subscribers connected to the LAN interface, such as panel PCs.

The diagram below represents a VPN connection. The client can be e.g. a PC or another industrial router, pre-configured for Internet access.

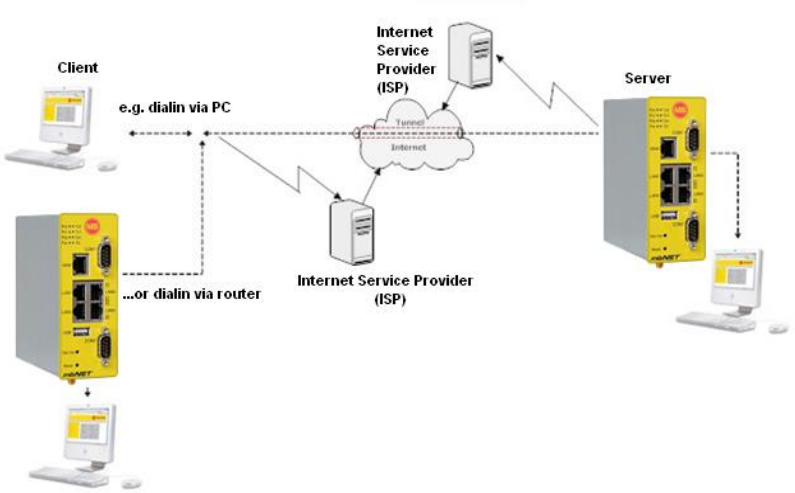


Figure 81

9.6.1 Connecting and configuring the router

9.6.1.1 Connecting the router

A VPN connection first requires that the router has an Internet connection in place. For instructions on how to configure the router for connection to the Internet, you can refer to the connection scenarios already described above, based on the connection mode required. As a basic principle, the router must be accessible via a public IP address.

9.6.1.2 Adding VPN dial-in users

- For a client to be able to dial into the industrial router via a VPN, a user must be added and have VPN dial-in rights assigned under user management. For instructions on exactly how to add a user with specific rights, please see section ***System – Users***.

IPSEC and PPTP

PPTP and IPSEC are the available protocols for a VPN connection tunneling protocol. The diagram below shows a VPN configuration using PPTP.

- **The connection wizard** helps you to configure your connections quickly and easily. To launch the wizard, click on the Wizards link at the top right of your browser. If you have disabled the autolaunch function for wizards, click on the Start button for the VPN connection wizard. Otherwise, check "VPN – set up a VPN tunnel" and ensure that everything else is unchecked.

Important: if you configured your Internet connection manually, the VPN wizard will display a warning. If you have not yet set up an Internet connection for the mbNET, please cancel the VPN wizard and set up an Internet connection first. Otherwise, check the box and click "Next".
Please note that with firmware versions 2.0 and higher, to enable IPSec configuration on the wizards page you first need to click on IPSec below the Start button for the VPN wizard, then on Save Changes, and Apply Changes.

Configuring the router for VPN connection to a client

9.6.1.3 Configuring the router (VPN server)

- On the home page, click on **VPN** in the navigation bar on the left and on **PPTP** in the navigation bar at the top.

- The following example should clarify the configuration. A description of the different configuration settings follows.

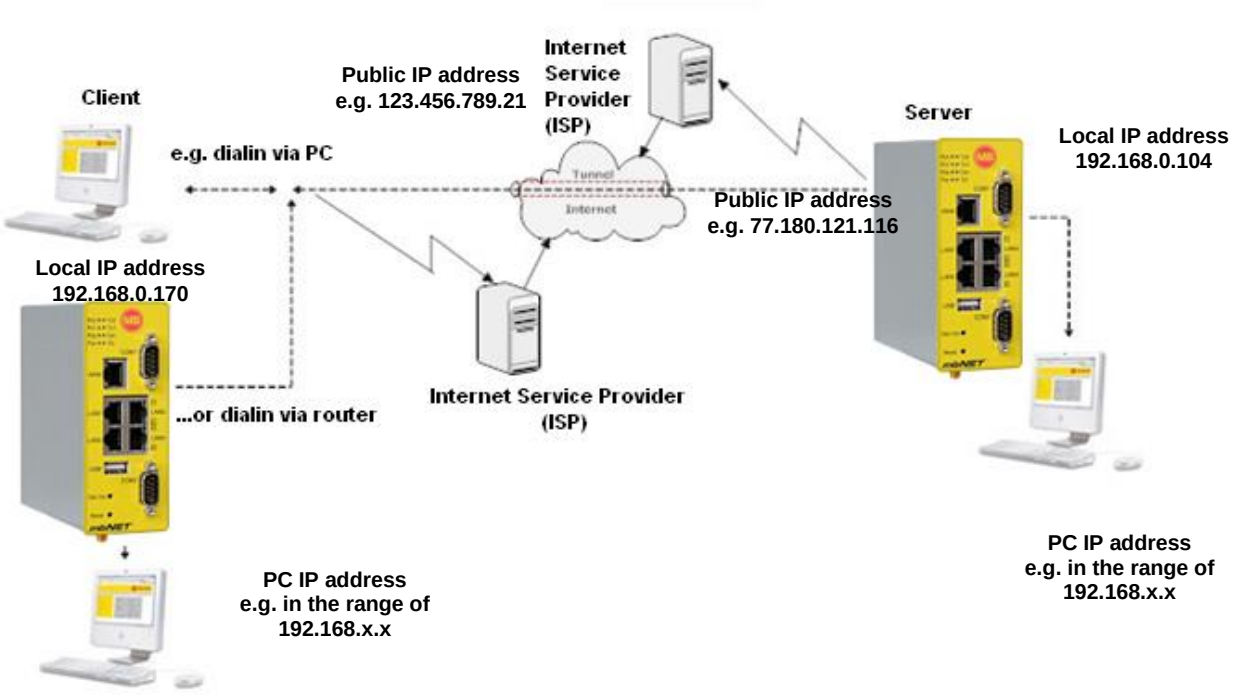


Figure 82

- Here, select "Connection between Networkclient and mbNET" and click "Next".
- Type in your key (PSK) and click "Next". Note that you should not use any special characters, and that your client must receive the key via a secure path.
- Now you can download a ready configured Windows VPN connection for your computer from the mbNET.

- To configure manually, proceed as follows:

  On the home page, click on **VPN** in the navigation bar on the left and on **PPTP** in the navigation bar at the top, then on the tab marked ***Server.***

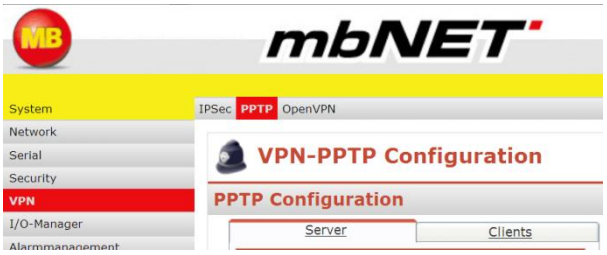


Figure 83

- This will display the screen below.

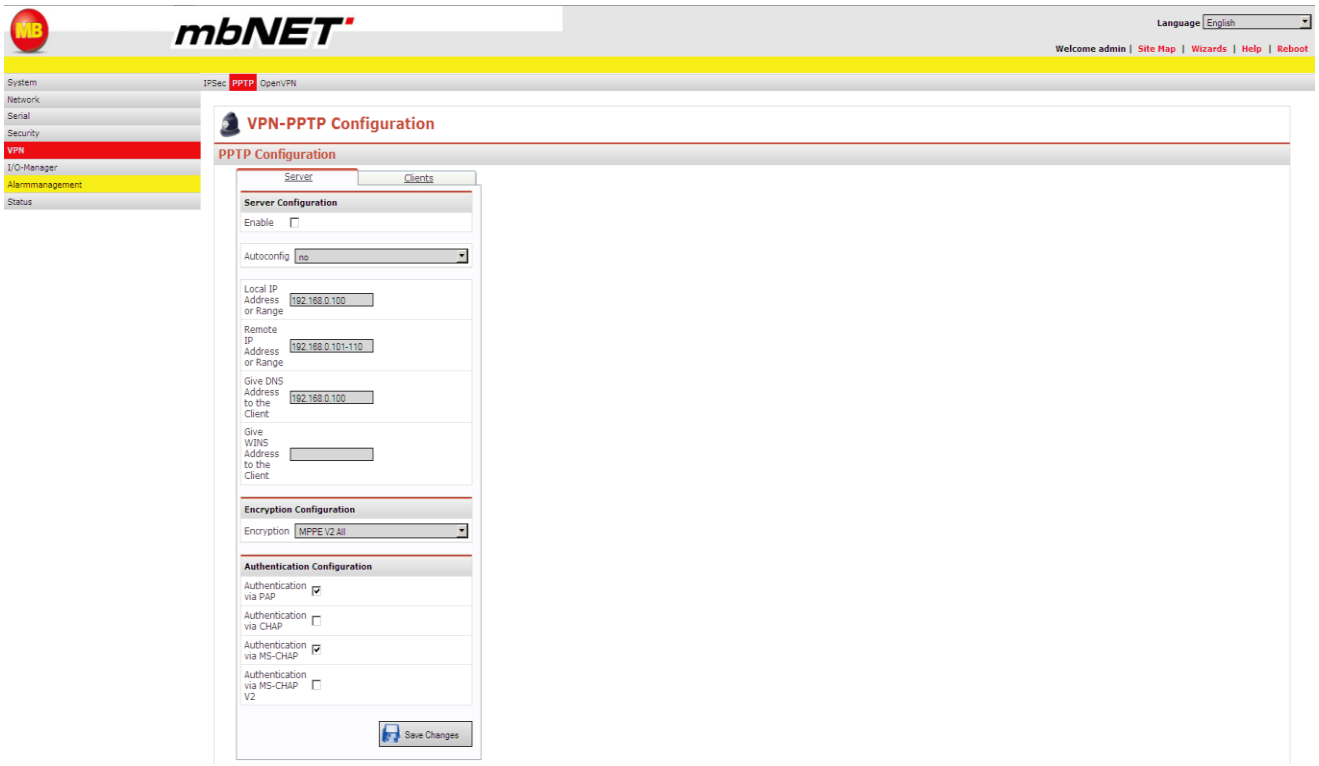
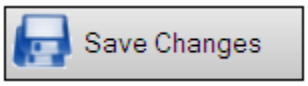


Figure 84

For a detailed description of the VPN – PPTP settings, please see section *VPN – PPTP*

Label	Description
Enable	To enable the connection, check the box by clicking on it.
Auto config	If you select "yes" here, the PPTP server will be configured using the mbNET's LAN address. This setting needs to be tried out first. You should only enter your PPTP server settings manually if there is an address conflict.
Local IP address or Range	Enter any local address in this input field. In the example it is: 192.168.10.100 Note: you can also use the router's LAN IP address. You should only re-host your PPTP server in a different address space if there is an address conflict.
Remote IP address or Range	Enter the remote addresses here. In the example: 192.168.10.160-170 This assigns the IP addresses of the connected clients within the range of 192.168.10.160 – 192.168.10.170. **Important** It is essential that the address or address range entered here is in the same address space as the local IP address chosen above
Give DNS Address to the client	Enter the DNS server address. In this case: 192.168.0.100 (router IP address)
Encryption	Use the default setting (MPPE V2 All)
Authentication	Use the default setting (via CHAP and MS-CHAP V2).

- ❑ Save your changes by clicking **Save Changes.**



- ❑ Finally, to save your changes permanently to the router, click **Apply Changes.**

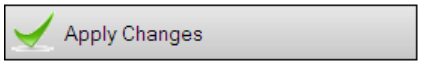


Figure 85

9.6.2 Configuring a client PC for a VPN connection to the router

- ❑ To proceed with set up, the client PC must have an existing Internet connection. For information on setting up a client PC please see section ***Configuring a client (PC) for router access***

- ❑ In Windows Control Panel, click on **Network Connections** and then on **Create a new connection.**

- ❑ In the wizard that appears, select **Connect to the network at my workplace.**

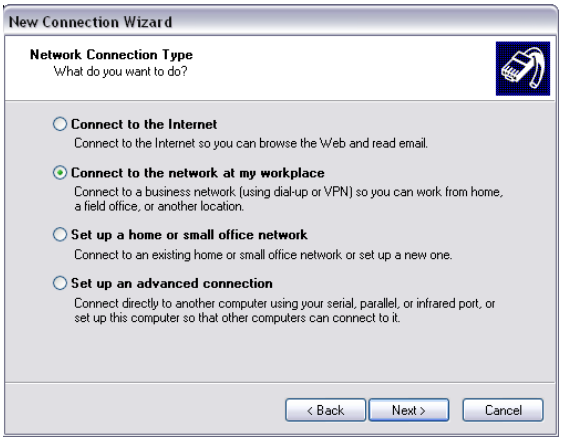

New Connection Wizard
Network Connection Type
What do you want to do?
Connect to the Internet
Connect to the Internet so you can browse the Web and read email.
Connect to the network at my workplace
Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.
Set up a home or small office network
Connect to an existing home or small office network or set up a new one.
Set up an advanced connection
Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it.
< Back
Next >
Cancel

Figure 86

- ❑ On the next screen, select **VPN connection.**

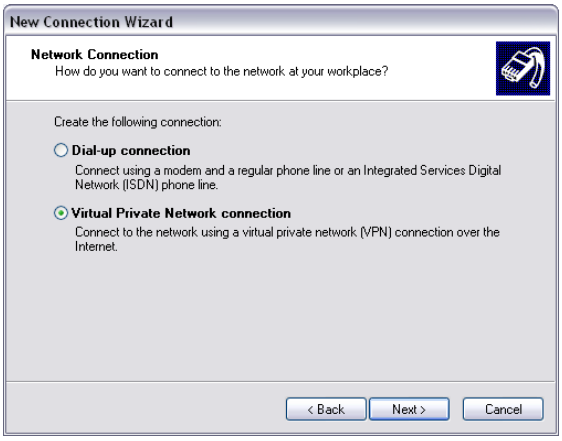

New Connection Wizard
Network Connection
How do you want to connect to the network at your workplace?
Create the following connection:
Dial-up connection
Connect using a modem and a regular phone line or an Integrated Services Digital Network (ISDN) phone line.
Virtual Private Network connection
Connect to the network using a virtual private network (VPN) connection over the Internet.
< Back
Next >
Cancel

Figure 87

- ❑ Now enter a name for the **VPN connection**.

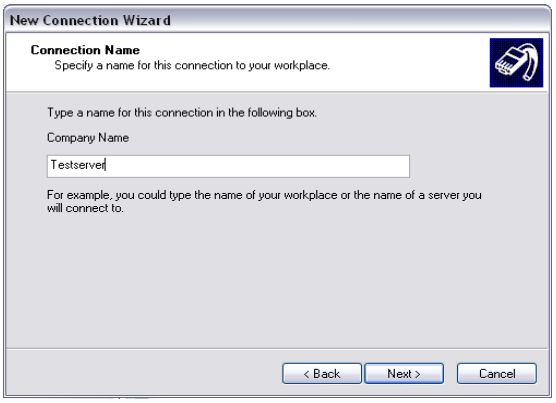

New Connection Wizard
Connection Name
Specify a name for this connection to your workplace.
Type a name for this connection in the following box.
Company Name
Testserver
For example, you could type the name of your workplace or the name of a server you will connect to.
< Back
Next >
Cancel

Figure 89

Setting up the router for a VPN connection (continued)

Configuring a client PC for a VPN connection to the router (continued)

- ❑ Here, enter either the DynDNS service forwarding name, or the current **IP address** of the router.

  ► *The example in Figure 86 uses an IP address assigned by the ISP.*

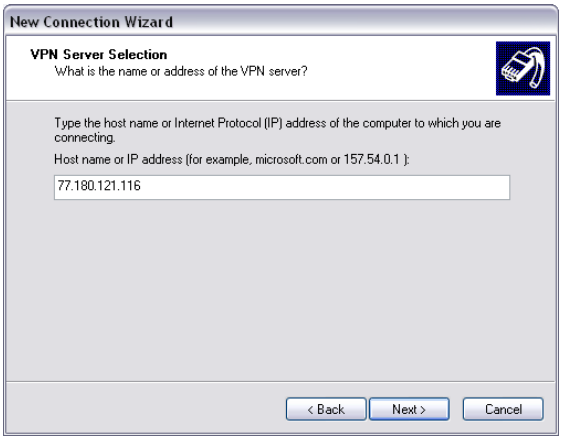

New Connection Wizard
VPN Server Selection
What is the name or address of the VPN server?
Type the host name or Internet Protocol (IP) address of the computer to which you are connecting.
Host name or IP address (for example, microsoft.com or 157.54.0.1):
77.180.121.116
< Back
Next >
Cancel

Figure 88

For information on setting up and using the MB Connect Line DynDNS service, please see section Network – DynDNS

When entering the router's IP address, make sure that you always enter the current IP address (the IP address changes every time the router connects to the Internet).

- ❑ You can now choose whether the connection will be available to all users or only to the current user.
- ❑ Now add a desktop shortcut to the connection.

  ✓ **The VPN connection is now set up.**

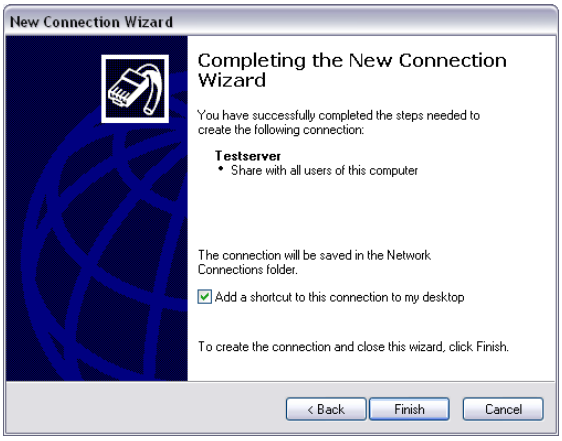

New Connection Wizard
Completing the New Connection Wizard
You have successfully completed the steps needed to create the following connection:
Testserver
• Share with all users of this computer
The connection will be saved in the Network Connections folder.
Add a shortcut to this connection to my desktop
To create the connection and close this wizard, click Finish.
< Back
Finish
Cancel

Figure 89

9.6.3 Setting up a VPN connection between client PC and router

9.6.3.1 Router Internet dial-in

- ❑ Depending on the connection mode, the router must be configured for Internet access, connected to the Internet, and accessible via the IP address.

9.6.3.2 Setting up a VPN connection from client to router

- ❑ Double-click on the VPN connection icon and in the next screen, enter the user name and password to which you assigned VPN dial-up rights in the router's user management settings.

Figure 90

9.6.3.3 Additional settings

- ❑ Double-click on the VPN connection icon and then click Properties. In the "Networking" menu tab you can set the VPN type to LT2P or PPTP. Select "PPTP VPN".

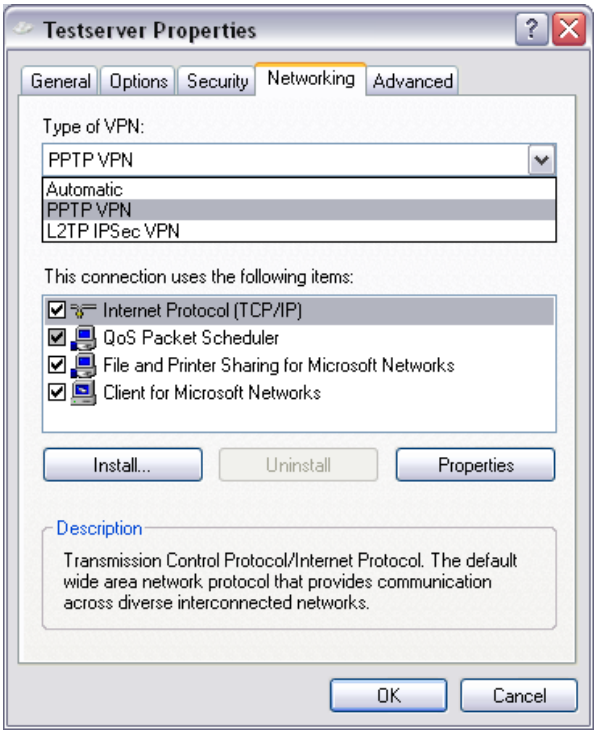


Figure 91

Setting up the router for a VPN connection (continued)

The client PC will display a flashing screen icon the router is connected. You can display the connection properties by right-clicking on the icon

On a PC connected to the router, clicking Status on the sidebar and VPN-PPTP on the navigation bar at the top will show you information on the current status of the VPN connection, such as users currently dialed in, or current connection status.

Where an industrial router has been set up as a client, please see the next section for settings that will allow it to access another remote industrial router.

9.7 Configuring a connection between two routers via VPN PPTP

- Instead of a client PC, you can also configure another router as a client. As a client, a router must be configured such that the router on the other end of the connection is its VPN server. Both routers need an Internet connection. For details of configuring the industrial router as a VPN server, please see the previous section ***Configuring the industrial router for a VPN connection with a client.***
- The following example should clarify the configuration.

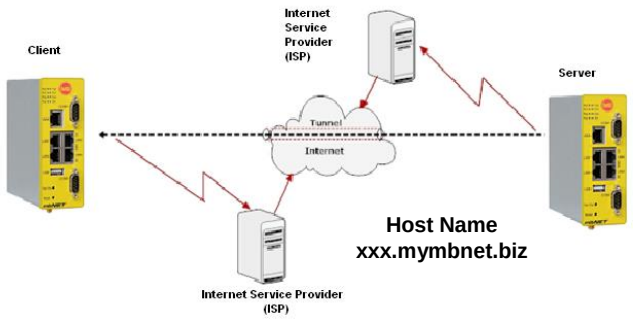
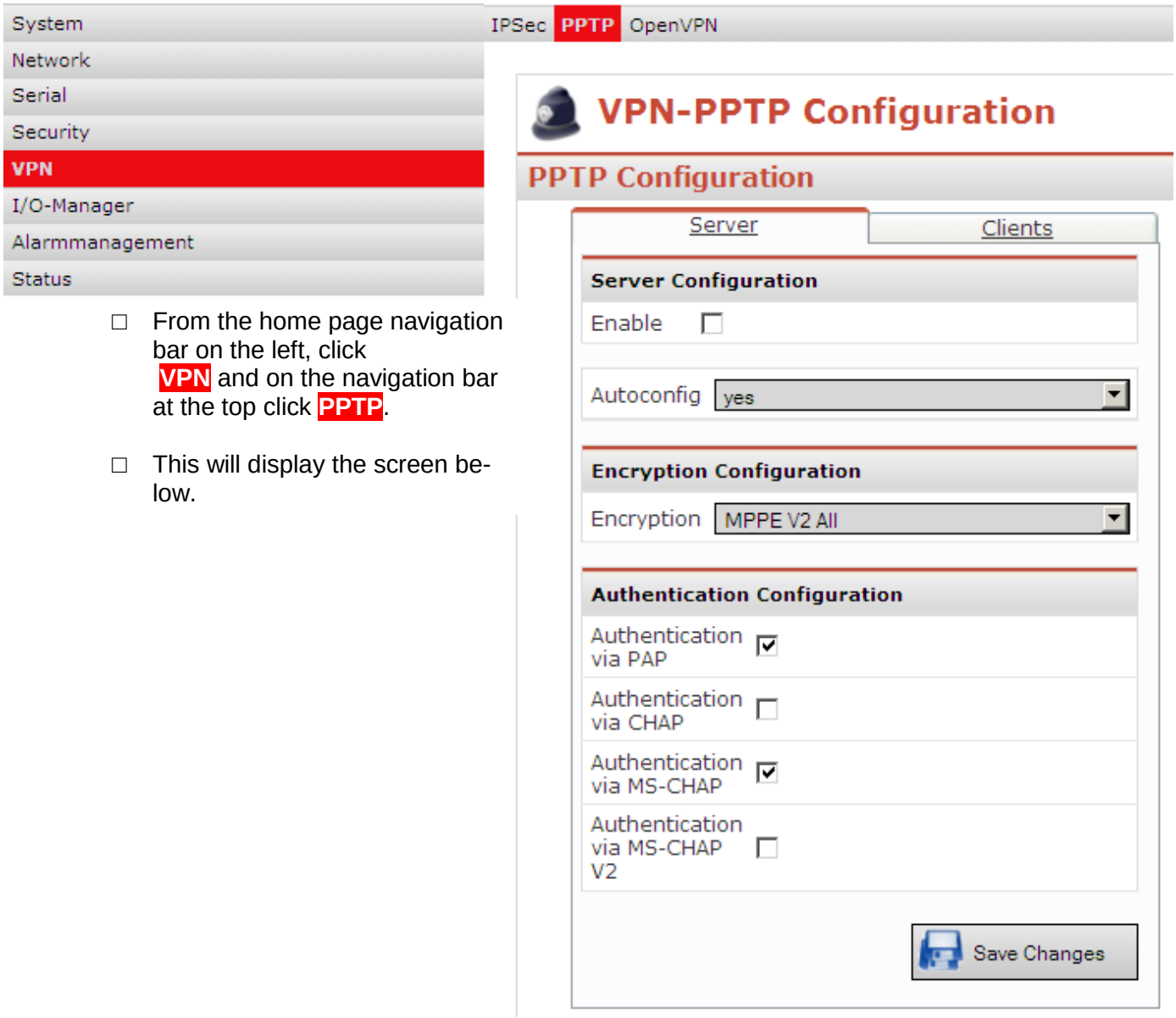


Figure 92

9.7.1 Settings for connecting two industrial routers – PPTP – server



- ☐ From the home page navigation bar on the left, click **VPN** and on the navigation bar at the top click **PPTP**.
- ☐ This will display the screen below.

Figure 93

If you now check the Enable box and save this setting, your server is live. It will then provide dial-in clients with addresses from its local network and use its LAN address as the PPTP server address.

If you wish to use other addresses,
set the "Autoconfig" option to NO and you will see the following screen:

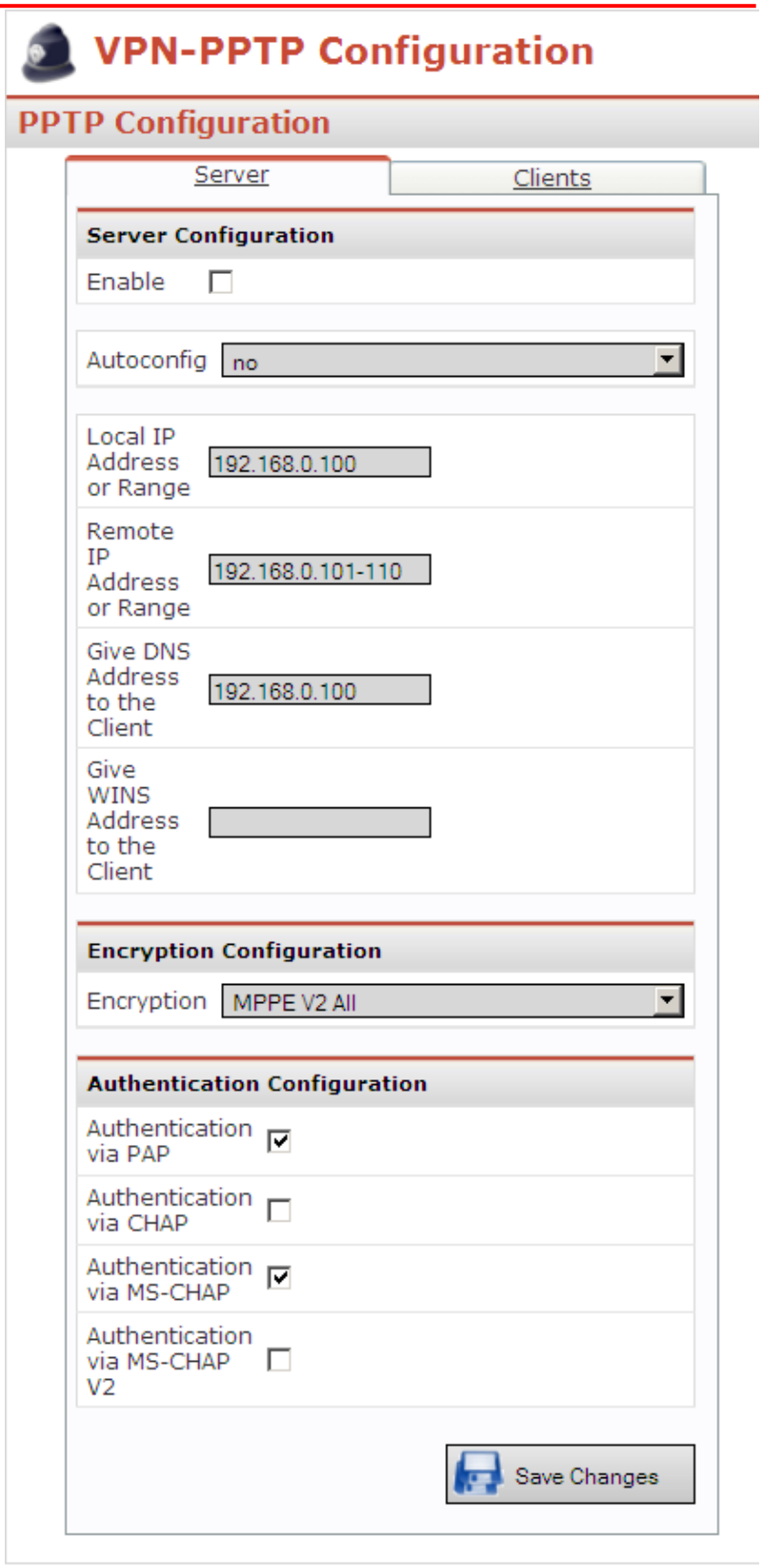


Figure 94

Label	Description
Enable	To enable the connection, check the box by clicking on it.

Auto config	Selecting "yes" means that the mbNET's local network range and IP address will be used. By selecting "no", you can enter this information manually.
Local IP address or Range	This is the PPTP server address
Remote IP address or Range	Enter the address or address range of dial-up clients here.
Give DNS address to the client	Here, enter the address of the server currently providing name resolution. Usually, you can enter the PPTP server address here.
Give WINS address to the client	The WINS server IP address can also be entered here for compatibility with older Microsoft operating systems.
Encryption	This option selects the type of data encryption. ☐ MPPE V2 All ☐ MPPE V2 128 ☐ MPPE V2 40 ☐ None **You should only select "none" if it is for test purposes. The data will not be transferred securely.**
Authentication via PAP, CHAP, MS-CHAP, MS-CHAP V2	You can select which authentication methods your PPTP server will support here. Place a check next to your chosen methods and click on Save Changes. Make sure that the client is also using one of the supported authentication methods, otherwise it will not be able to connect.

Note that when using MPPE encryption,
you must ALWAYS use MS-CHAP or MS CHAP v2 as the authentication method**.**

For more detail on VPN – PPTP please see section *VPN – PPTP*

9.7.2 Settings for connecting two industrial routers – PPTP – Clients

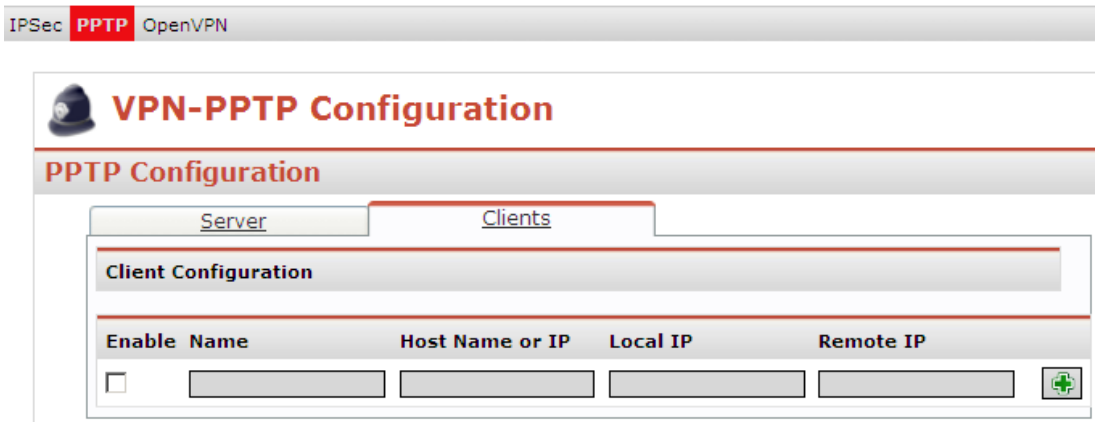


Figure 95

Clicking on the green plus sign on the far right will open the following configuration screen.

- ☐ Enter a name of your choosing for the connection.
- ☐ Next, you need to enter the public address or DynDNS name for the PPTP server.
- ☐ For "Local IP", you can use the PPTP server address. Generally speaking, this field should be left blank, as the PPTP server sends its address when it establishes a connection.
- ☐ For "Remote IP", you can enter a single address or a whole network. We recommend using the settings shown in the screenshot on the right, and entering a network address. This makes the network accessible to all subscribers.
  Please note that the network address must be in CIDR notation as shown in the screenshot on the right (192.168.0.0/24)
- ☐ For Authentication, choose one of the methods supported by the PPTP server. You can see what these are by looking on the PPTP server's web page, under VPN-PPTP.
- ☐ Use the same type of encryption as the server. Please note that when using MPPE encryption, you must always enable MS-CHAP or MS-CHAP V2 authentication.
- ☐ For the User and Password fields, the user must have been added to the PPTP server (e.g. standard user name ADMIN, without password). However you can add a new user to the server (to do this you need to change the user on the server web page under System Users).
- ☐ The final option allows you to choose which events the client should connect for. The following options are available:
  - Connect immediately
  - Connect on traffic
  - Connect on signal high at input 1-4

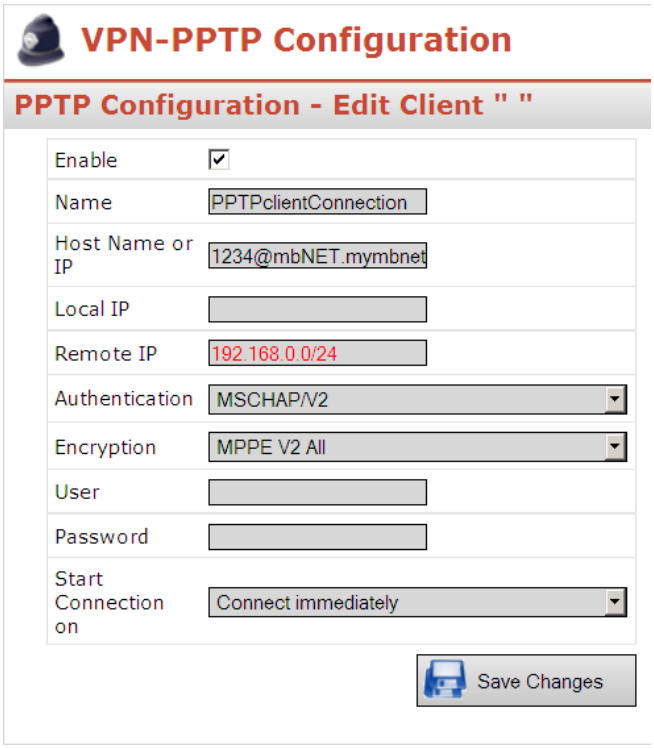


Figure 96

❑ Save your changes by clicking **Save Changes.**

❑ Finally, to save your changes permanently to the router, click **Apply Changes.**

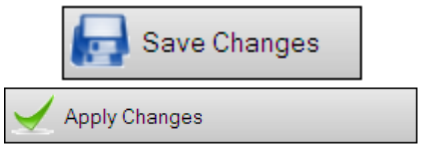


Figure 97

For more information on VPN – PPTP settings, please see section *VPN – PPTP*

Label	Description
Enable	To enable the connection, check the box by clicking on it.
Name	Assign a name to the client. In the example we used: PPTPclientConnection
Host name or IP	Here, enter the name or IP address that the client uses to contact the server. In the example, this is: 123456789@mbNET.mymbnet.biz
Local IP	The server address can be entered here. Generally speaking, this field can be left blank.
Remote IP	Enter the address of the remote station, or the address for a whole network. We recommend entering a network address. In the example: 192.168.0.0/24. Note the CIDR notation (/24 after the network address)
Authentication	Select an authentication method that is also enabled in the server settings.
Encryption	We recommend selecting MPPE V2 encryption. Note that if you select "none", your data will NOT be sent securely.
User & Password	Enter the user name and password of a user who has been added to the PPTP server as a system user (e.g. ADMIN, without password).
Start connection on	Select **Keep connection**. A connection will be established on restart or boot up. It is also possible to start the connection only for specified events.

.

10. Creating certificates and revocation lists using XCA.

10.1 Certificates overview

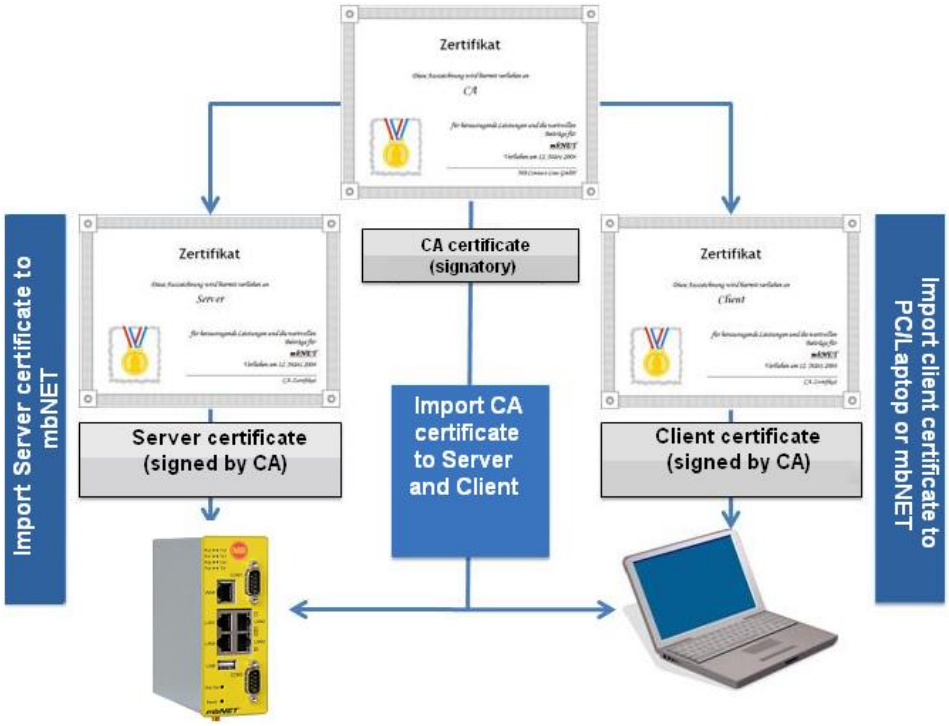


Figure 98

Any subscriber communicating over a VPN connection needs 2 certificates. One certificate must be signed by a CA (Certificate Authority). Each subscriber must have the CA certificate plus a "server" or "client" certificate. In our case, the server may be the mb*NET* or a separate server. The client is either a computer or another mb*NET*. The certificates are required to set up a secure VPN tunnel and are used to authenticate the VPN subscriber. If the subscriber has no certificate, or an invalid certificate, no VPN tunnel can be established between the two devices if the authentication setting on the mb*NET* is "X.509".

To understand how to create certificates, please see the next section.

10.2 Creating certificates

Christian Hohnstädt's XCA freeware program is useful for creating certificates. Using this program makes it easy to create X.509 certificates as well as the necessary private keys.
You can download the program from http://sourceforge.net/projects/xca free of charge, and install it in Windows in the usual way (run the `.exe` file).

When you launch XCA for the first time, a new database has to be created to manage the certificates. To do this, click "File" and then "New DataBase"

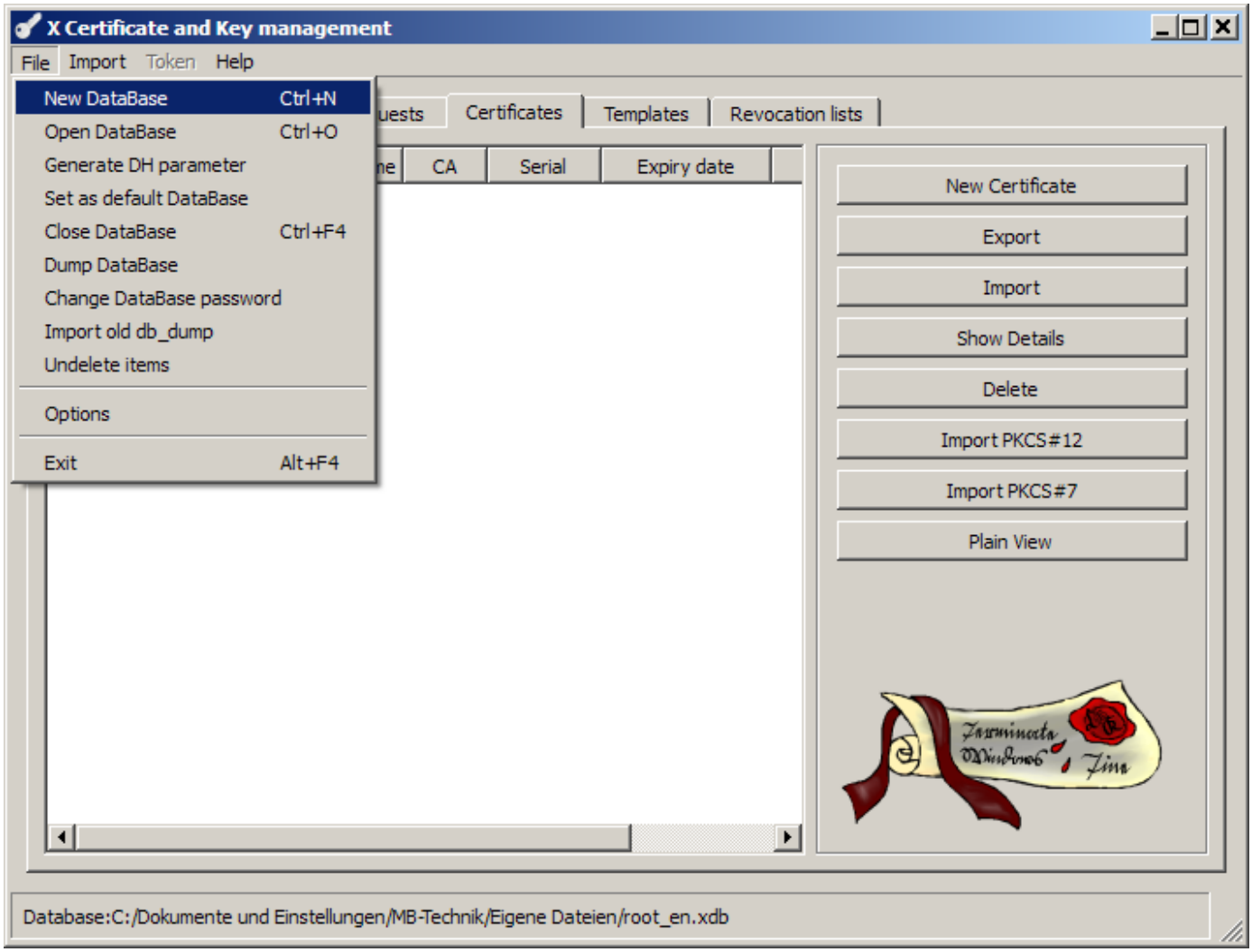


Figure 99

After choosing a name, file save location and password for the database, you can open it and start creating a root (CA) certificate.

10.2.1 Creating a root certificate

To create a root certificate, click on the *"Certificates"* tab and open the following dialog box by clicking *"New Certificate"*.

10.2.1.1 **Root certificate source**

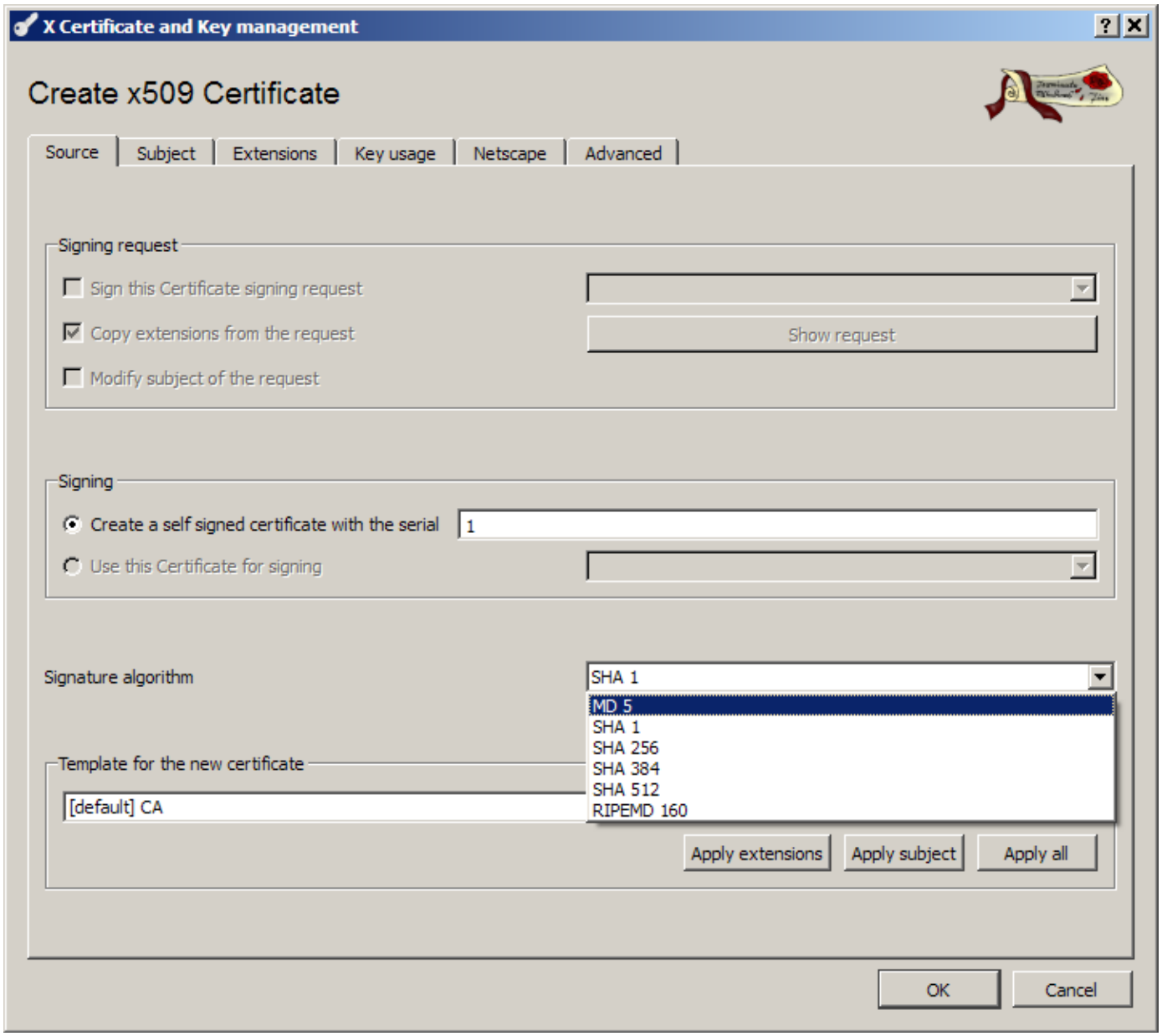


Figure 100

First, change the Signature algorithm to MD5 so that the certificate is compatible with the *mbNET*. Then you can go straight to the *"Subject"* tab and create the certificate.

10.2.1.2 Root certificate subject

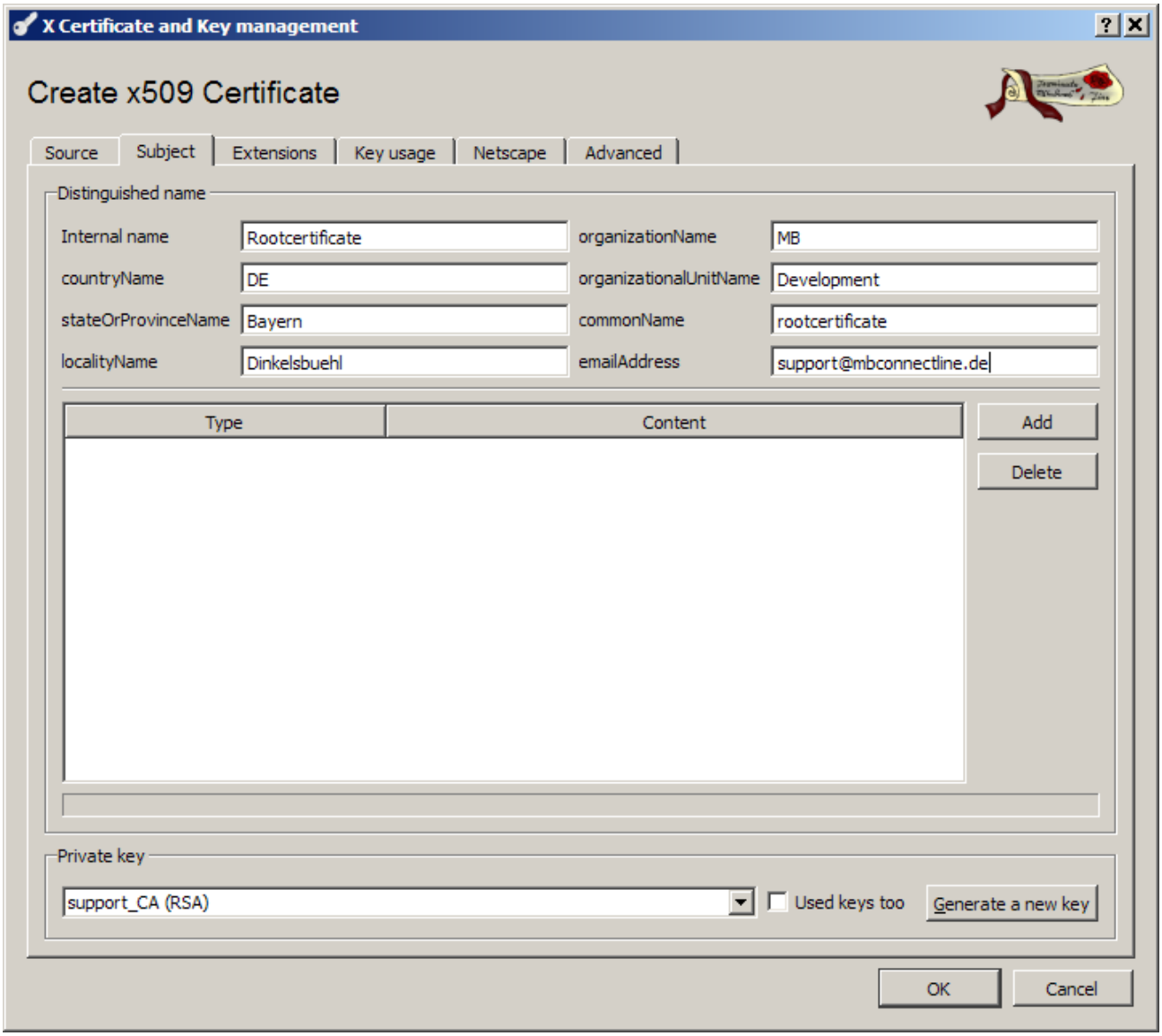


Figure 101

In the *"Subject"* tab, fill in the fields from "Internal Name" through "emailAddress". For VPNs using IPSec, Subject settings can later be used as an ID (cf. section Authentication)
Next, create a private key by clicking on *"Generate a new key"*.

Please do not use accents (e.g. ü) (Example: Dinkelsbuehl instead of Dinkelsbühl in the locality field)

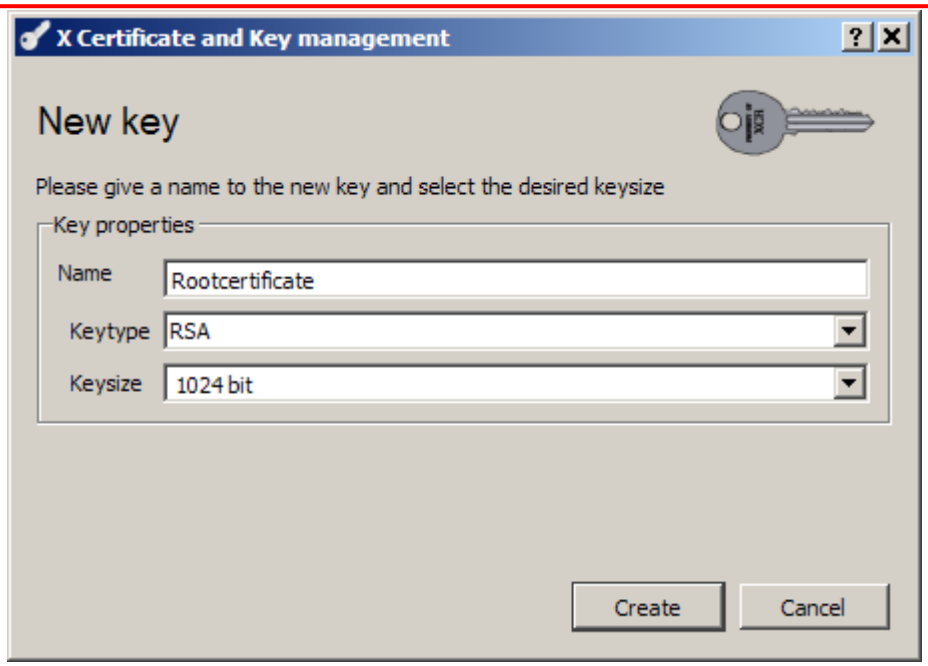


Figure 102

Select key type RSA. You can select any key size and of course, any name. The longer the key, the more secure the encryption but also the more processing power required.

10.2.1.3 **Root certificate extensions**

In the "Extensions" tab you will find the settings for certificate type and validity.

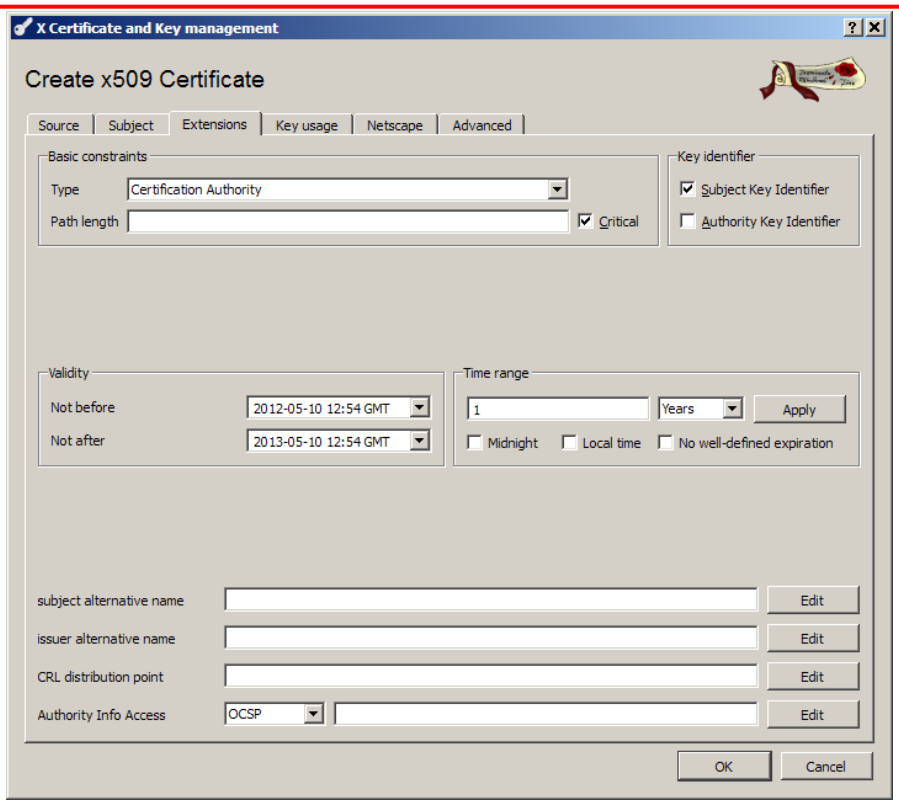


Figure 103

Basic constraints
Type = Certificate Authority (CA)
Check the box labeled Critical

and Key identifier
Check the box labeled Subject Key Identifier

Validity
You can enter a specific start and end date in the relevant fields or use the adjacent Time Range field.

Time Range
In the dialog boxes to the right, enter the number of days, months or years. The list below specifies how long individual certificates should be valid for:

- Personal certificates should be valid for 1 year.
- Server (SSL) certificates, 1 year.
- Router certificates should be valid for 1 year (external routers) or 10 years (internal routers).
- CA certificates should have an extended lifespan (e.g. >10 years).

Click *"Apply"* to confirm the **Time Range** values.

Subject alternative name
The subject alternative name is a list of alternative names for the certificate holder. These can be RFC822 names (email), DNS names, X.400 addresses, EDI names, URIs or IP addresses. In principle, any structured naming system is applicable. If using PKIX, this extension is essential when the certificate subject field is empty.

Issuer alternative name
For issuer alternative names, the same applies as for subject alternative names.

CRL distribution point
To be able to use a public access point for certificate revocation lists, you need to enter the LDAP or HTTP address of the list. The address should always be prefixed with a **URI** (universal resource indicator) (e.g. URI:http://de.wikipedia.de). For the field separator, use a colon. If you hold local revocation lists, this option is not relevant.

Authority Info Access
This PKIX extension defines how to access additional information and services from the issuer of the certificate. It can then provide more information about the CA (additional guidelines, root certificates ...) or online verification services (e.g. OCSP). Primarily, where certification applications like secure mail (S/MIME) do not return the entire certification path, using this extension in the end certificate is helpful for showing the verifying application where to retrieve the next higher level CA certificate.

10.2.1.4 Root certificate key usage

In the *"Key usage"* tab you will find key usage and extended key usage options. Neither key should be critical i.e. you should leave the boxes marked Critical unchecked.

To create a root certificate, please select the following values in the left hand column:

- Certificate Sign
- CRL Sign

Selecting these options means that your root certificate can sign the client certificate and revocation lists.

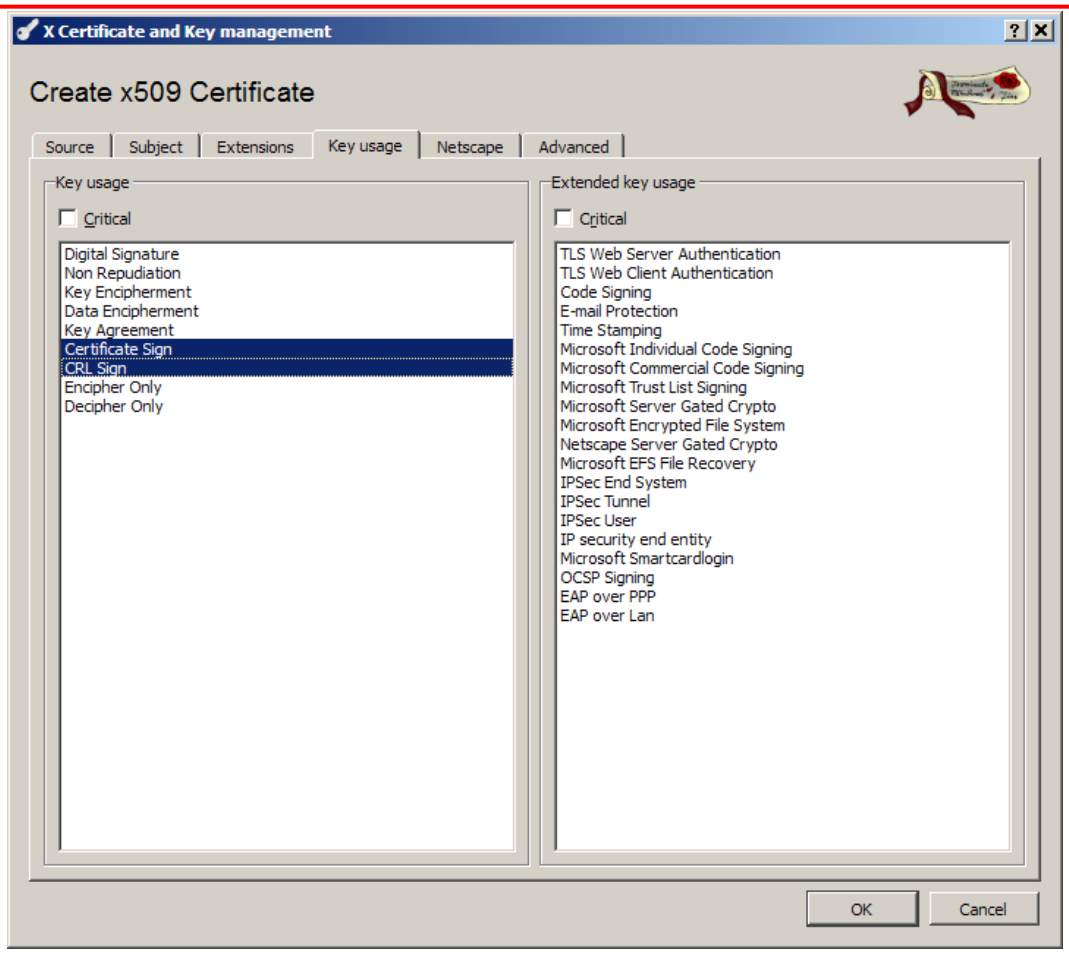


Figure 104

Now click on *"OK"* to complete root certificate creation.
Your root certificate is now ready and you can now derive and sign your additional certificates.

10.2.2 **Creating a client certificate**

To create a certificate signed by this CA, in the *"Certificates"* tab, highlight the root certificate that you just created, and click again on *"New Certificate"*.

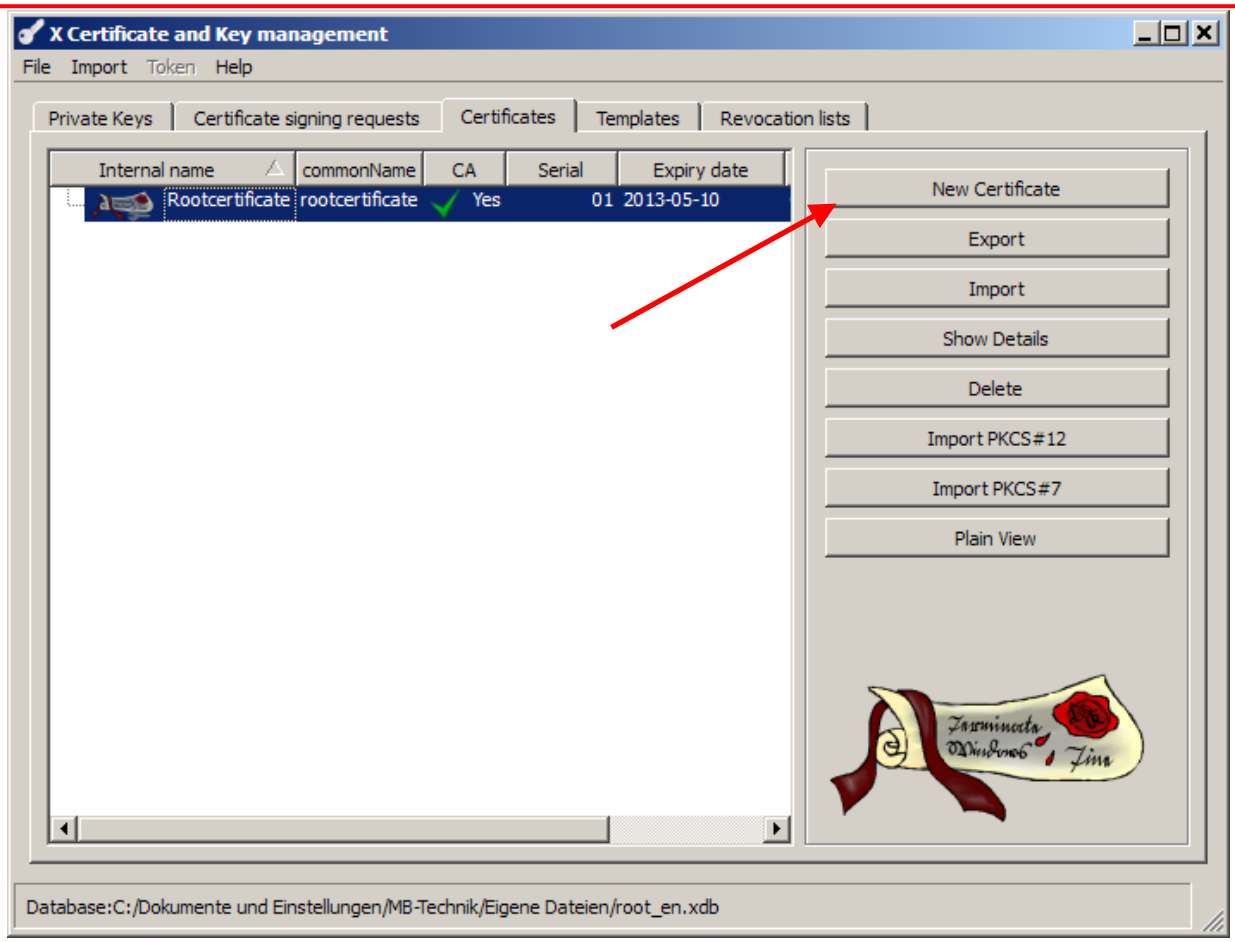


Figure 105

The dialog box below will appear.

10.2.2.1 Client certificate source

First we need to select our root certificate as the one that will be used as signatory. We also need to set the signature algorithm to MD5 again.

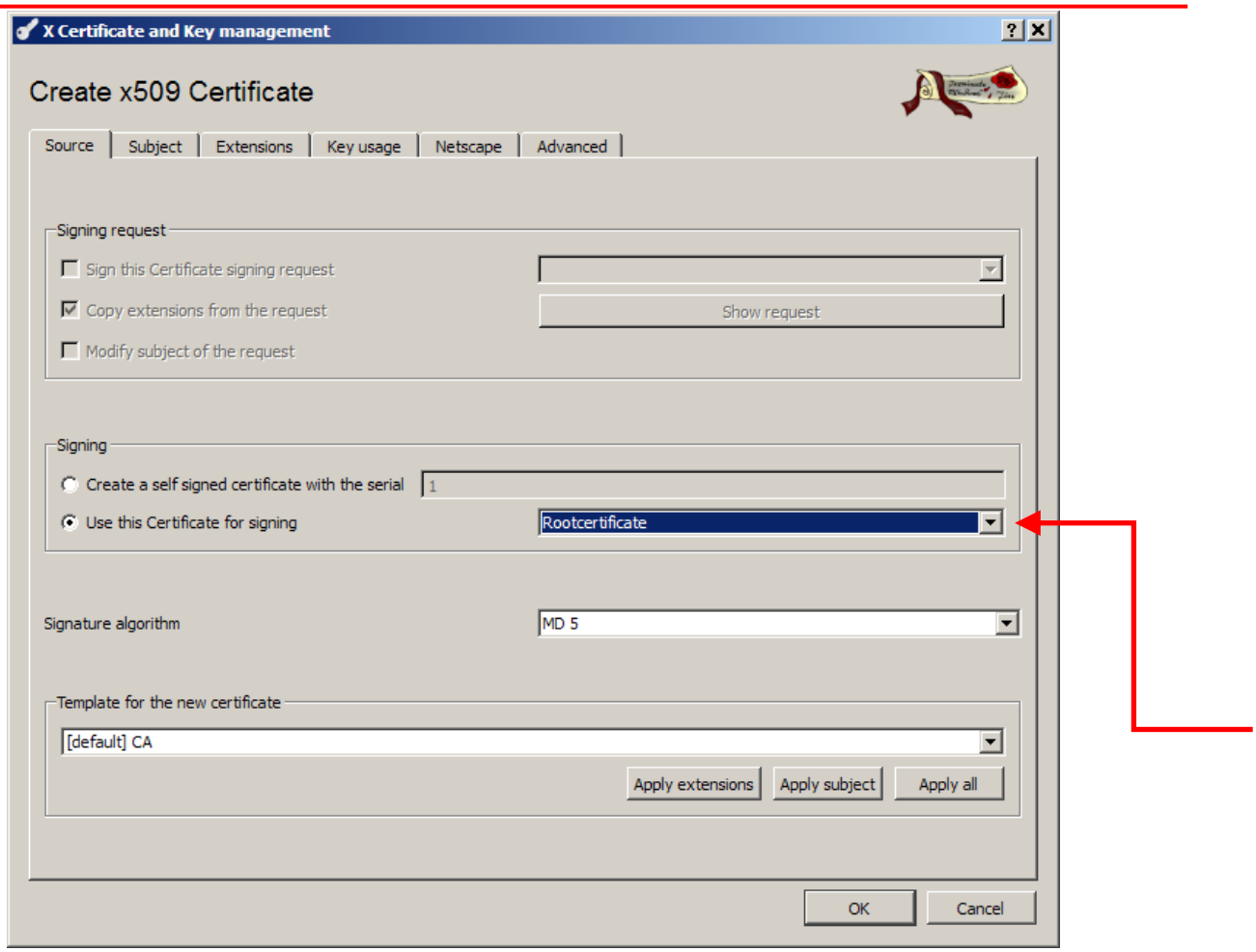


Figure 106

We see here that our root certificate is already set as the one to use as signatory.

10.2.2.2 **Client certificate subject**

Once again, assign the client certificate details, from Internal name through emailAddress.

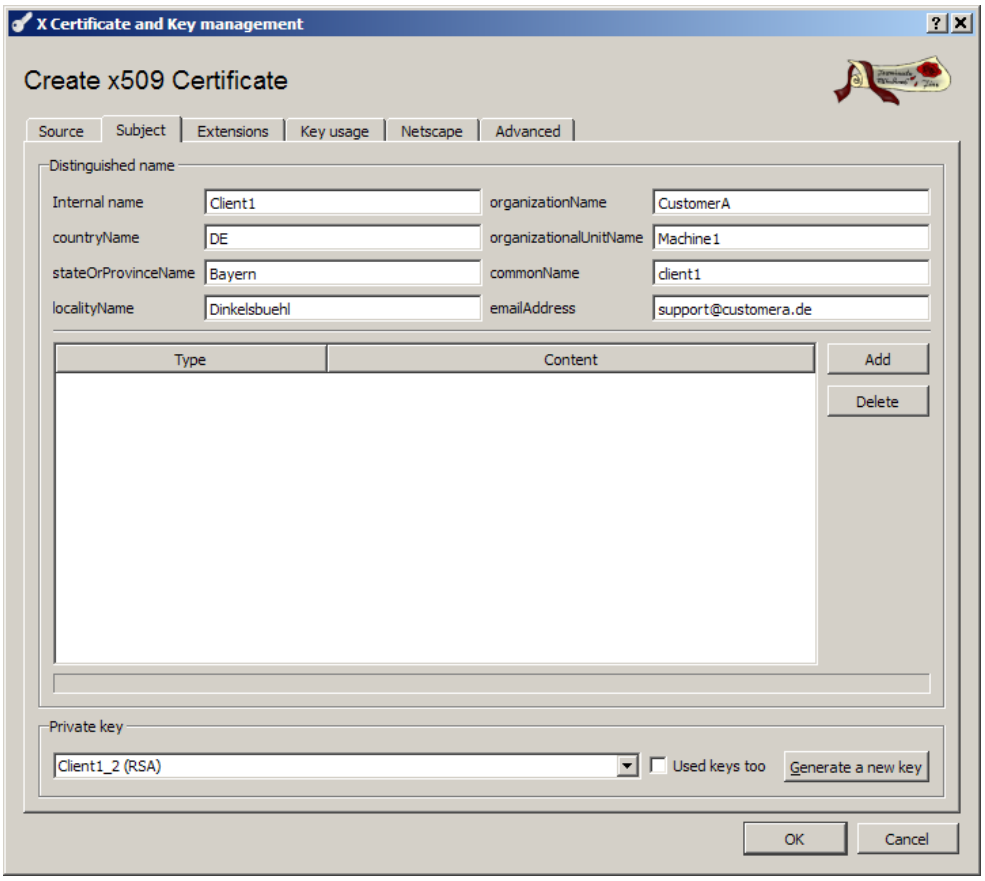


Figure 107

Then generate a key for the client certificate. It is recommended that the key should be the same size as the one for the root certificate.

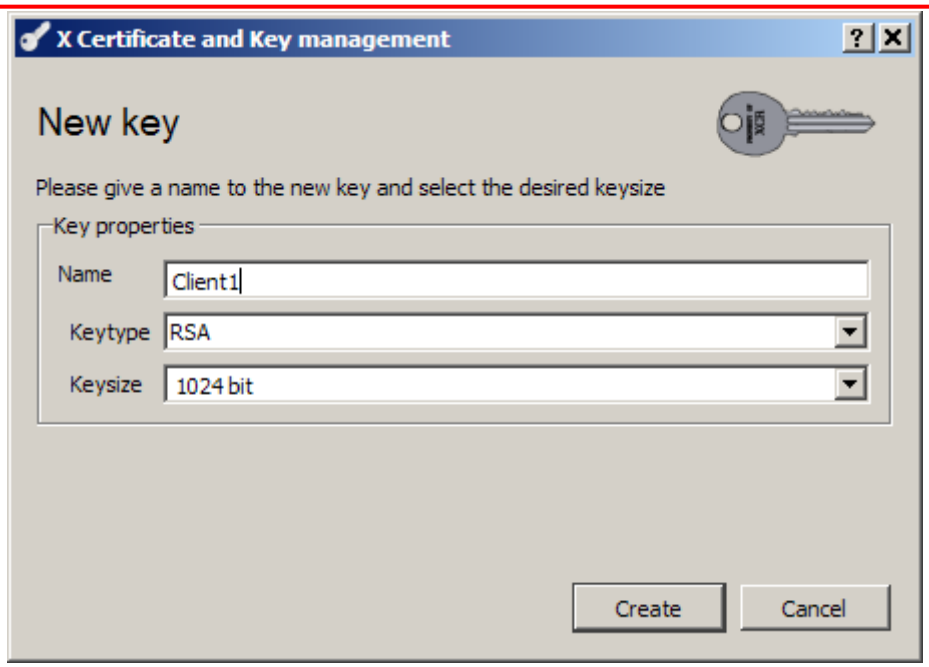


Figure 108

10.2.2.3 **Client certificate – Extensions**

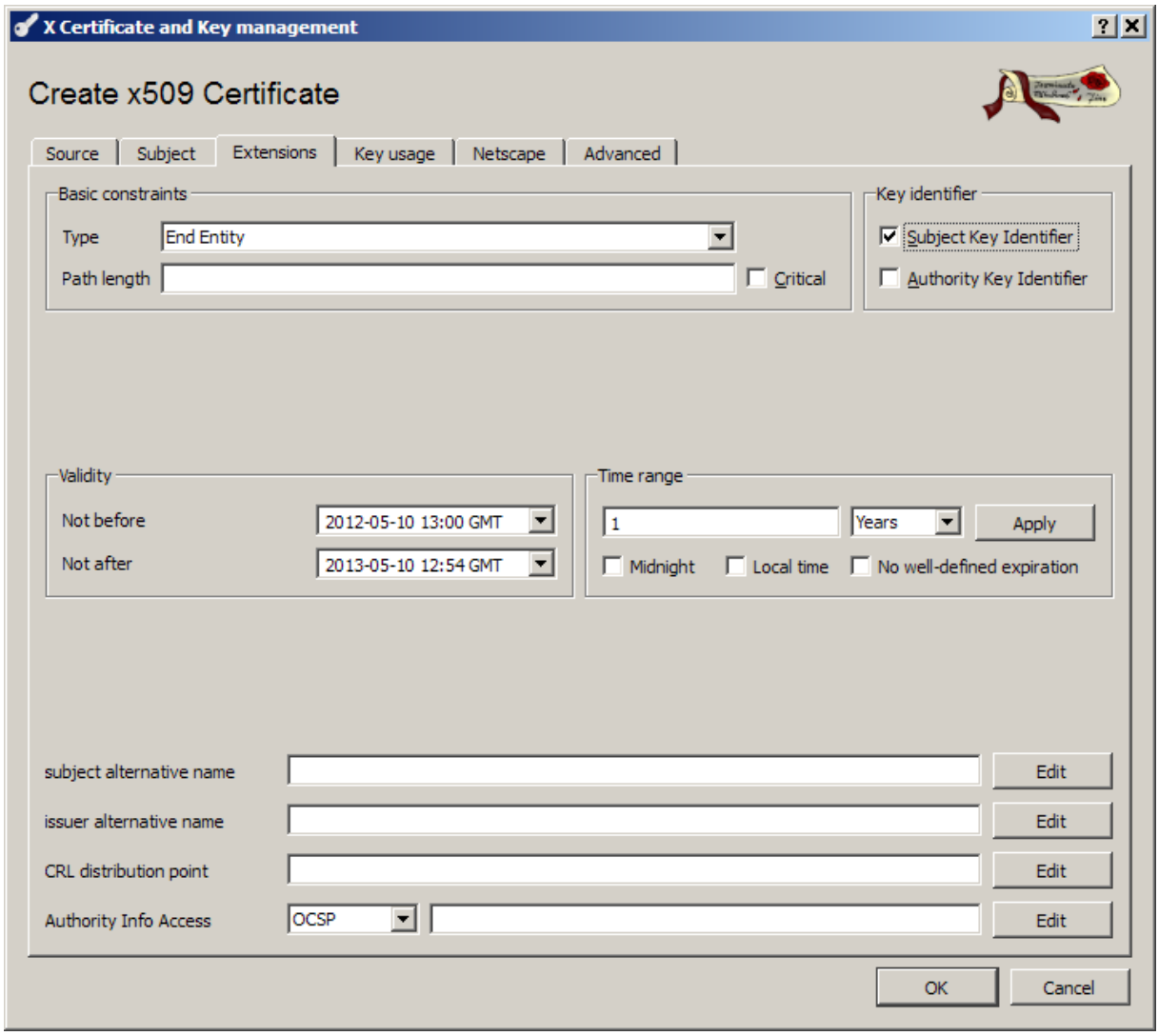


Figure 109

As your client certificate does not need to sign any other certificate, select End Entity as the Certificate Type.

Basic constraints
Type = End Entity

Key identifier
Check the box labeled Subject Key Identifier

Validity
You can enter a specific start and end date in the relevant fields or use the adjacent Time Range field.

Time Range
In the dialog boxes to the right, enter the number of days, months or years. The list below specifies how long individual certificates should be valid for:

- Personal certificates should be valid for 1 year.
- Server (SSL) certificates, 1 year.
- Router certificates should be valid for 1 year (external routers) or 10 years (internal routers).
- CA certificates should have an extended lifespan (e.g. >10 years).

Click *"Apply"* to confirm the **Time Range** values.

Subject alternative name
The subject alternative name is a list of alternative names for the certificate holder. These can be RFC822 names (email), DNS names, X.400 addresses, EDI names, URIs or IP addresses. In principle, any structured naming system is applicable. If using PKIX, this extension is essential when the certificate subject field is empty.

Issuer alternative name
For issuer alternative names, the same applies as for subject alternative names.

CRL distribution point
To be able to use a public access point for certificate revocation lists, you need to enter the LDAP / or HTTP address of the list. The address should always be prefixed with a **URI** (universal resource indicator) (e.g. URI:http://de.wikipedia.de). For the field separator, use a colon. If you hold local revocation lists, this option is not relevant.

Authority Info Access
This PKIX extension defines how to access additional information and services from the issuer of the certificate. It can then provide more information about the CA (additional guidelines, root certificates ...) or online verification services (e.g. OCSP). Primarily, where certification applications like secure mail (S/MIME) do not return the entire certification path, using this extension in the end certificate is helpful for showing the verifying application where to retrieve the next higher level CA certificate.

10.2.2.4 **Client certificate – Key usage**

If you create a client certificate as an end entity, you do not need any of these optional settings. You can proceed straight to the next tab.

10.2.2.5 **Client certificate – Netscape**

If you would like additional security, you can also select the SSL Server or SSL client option for your VPN subscribers according to their role (client or server).
The advantage of this is that OpenVPN can query whether a VPN server is also equipped with SSL. This option can also be enabled on the mbNET. The section on OpenVPN

goes into more detail on this, and on the settings options. If you set up your certificate with both elements, it can be used with a VPN client or a VPN server.

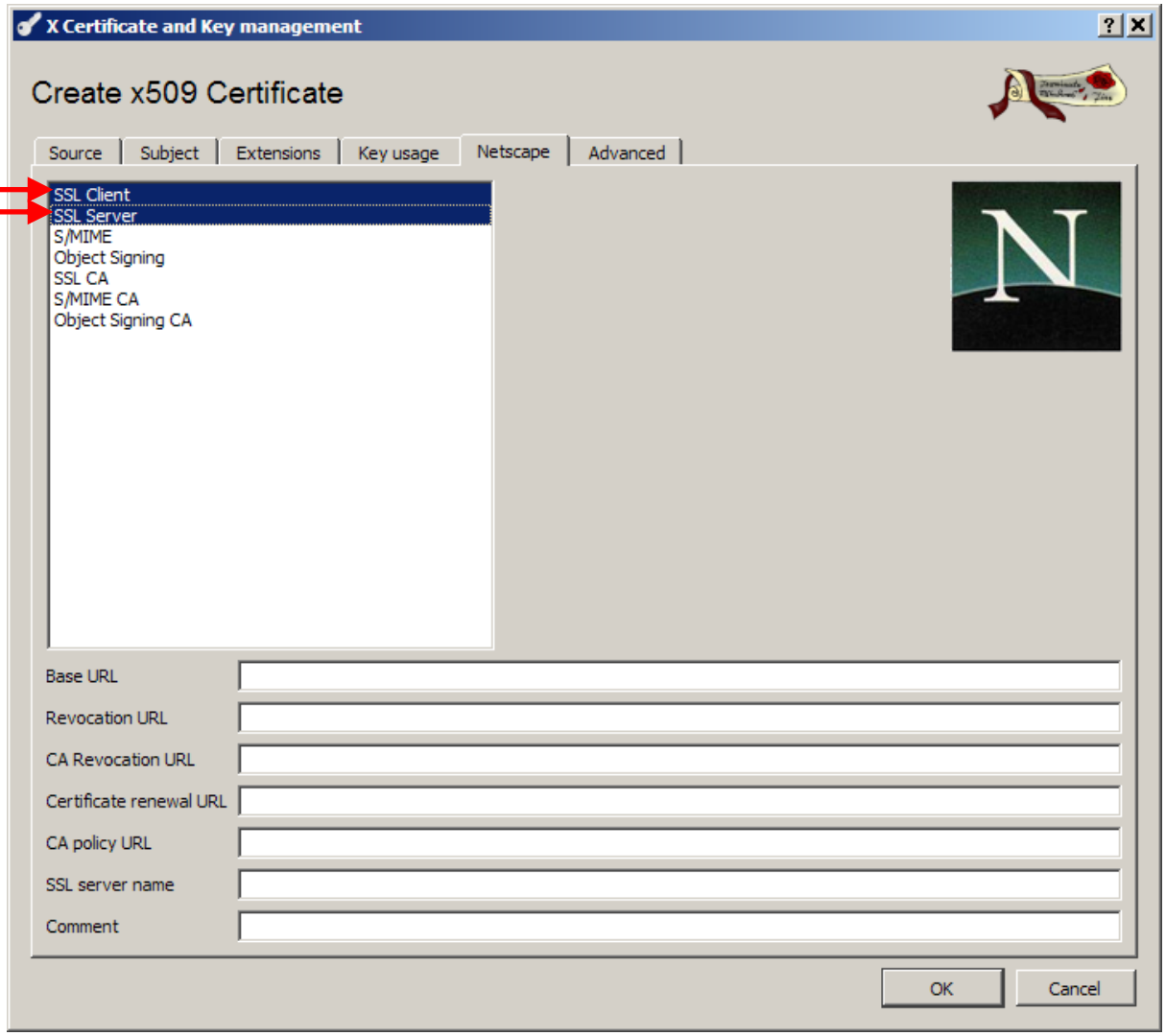


Figure 110

In the *"Netscape"* tab, no IPSec settings are required.
If using OpenVPN with "Peer must be TLS server" enabled, select only the SSL Server option. See also the screenshot above.

Now the certificates need to be published by highlighting the relevant ones in the *"Certificates"* tab and then clicking *"Export"*.

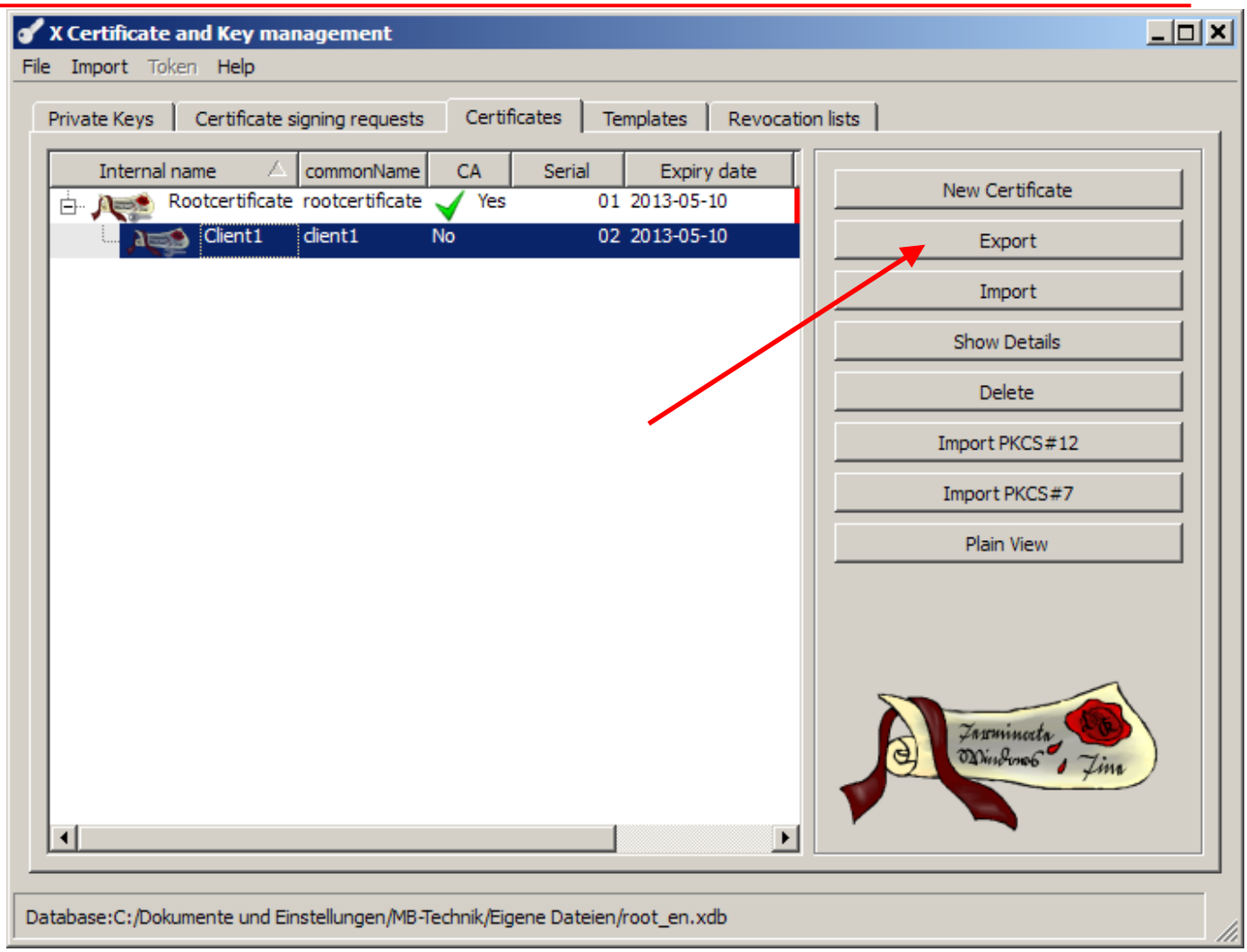


Figure 111

In the menu below, you can specify the save location for the certificate on your computer, and also the file format.

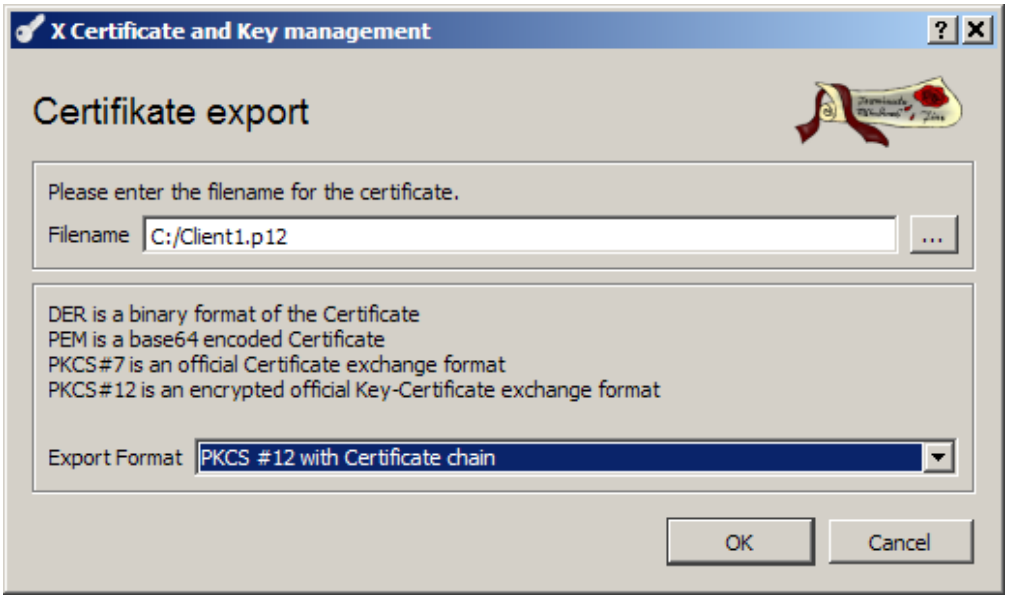


Figure 112

As your client is to be authenticated by the client certificate, it also needs the private key for this certificate. As shown in Figure 112, export the client certificate using export format PKCS #12 with Certificate chain. When you click OK, the client certificate will save to the location that you specified above. The client certificate then has the file extension .p12.

You must use the PEM (file extension .crt) format when exporting the root certificate.

These certificates can then be imported to the *mbNET* router via the web interface (cf. section **System – Certificates**).
For an explanation of how to set up these certificates for a Windows client, see **Importing certificates in Windows XP**.

10.3 Creating CRL files (revocation lists)

If you wish to withdraw a team member's rights to use the VPN tunnel, please read this section and create a certificate revocation list.
To do this, re-open XCA. Open the database containing your team member's certificate. To confirm a certificate as invalid, right-click on it and the dialog box below will appear:

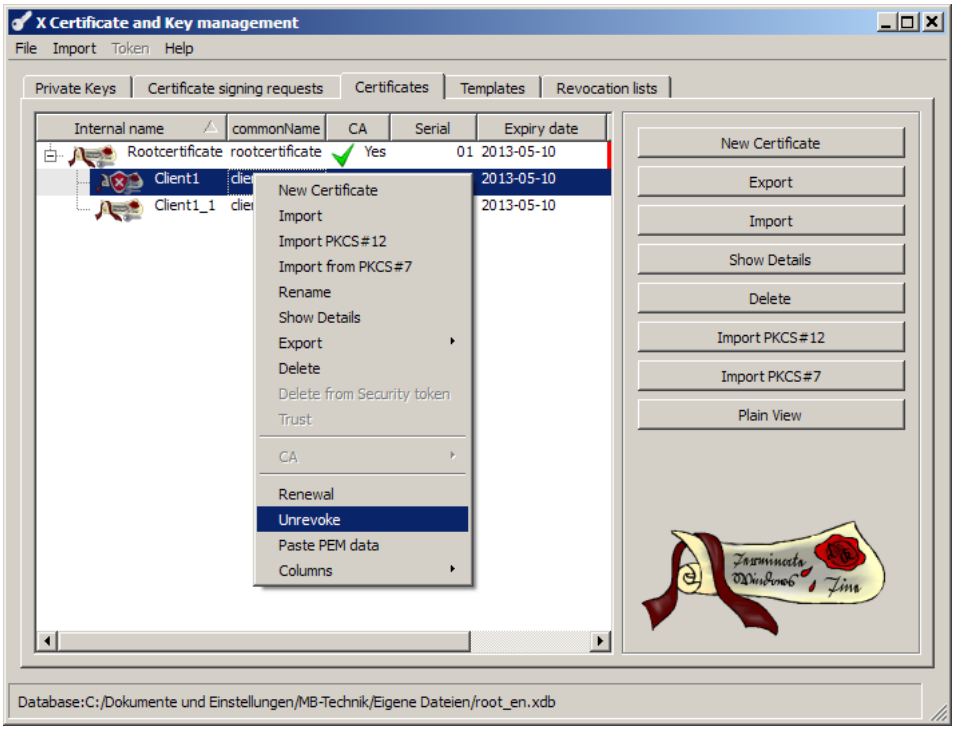


Figure 113

Clicking on *"Revoke"* flags the relevant certificate with a red X, and it is no longer valid. To remove the flag and make the certificate entry valid again, click on "Unrevoke" as shown in the screenshot.

Next, right-click on the associated root certificate. The following dialog box will appear:

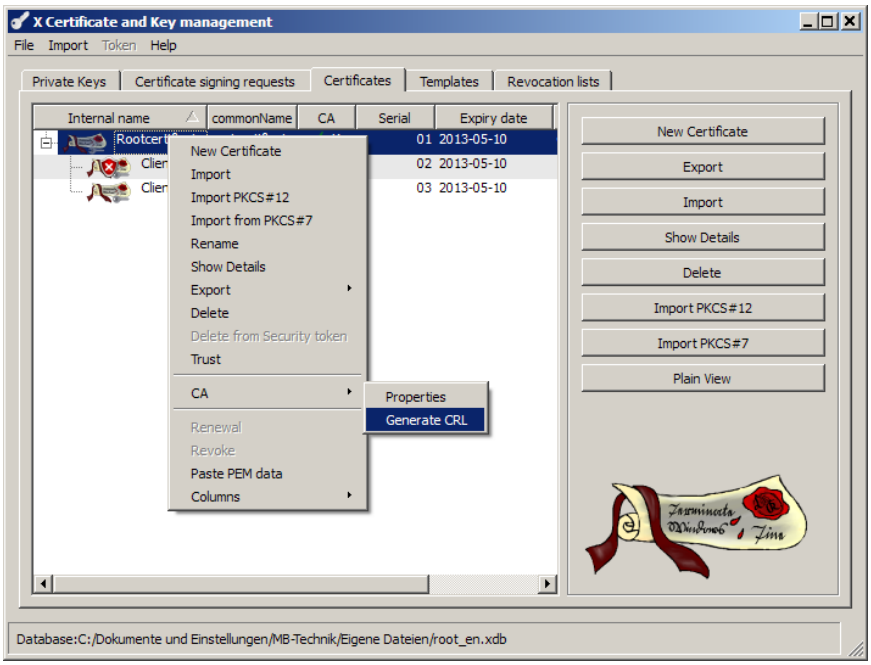


Figure 114

You can create a revocation list here using *"CA → Generate CRL"*, as shown in the screenshot above. Please ensure that under "hash algorithm", you also select MD5. There are no check boxes to enable for extensions. The CRL must now be exported, and then imported to the mbNET. To export, proceed as follows:

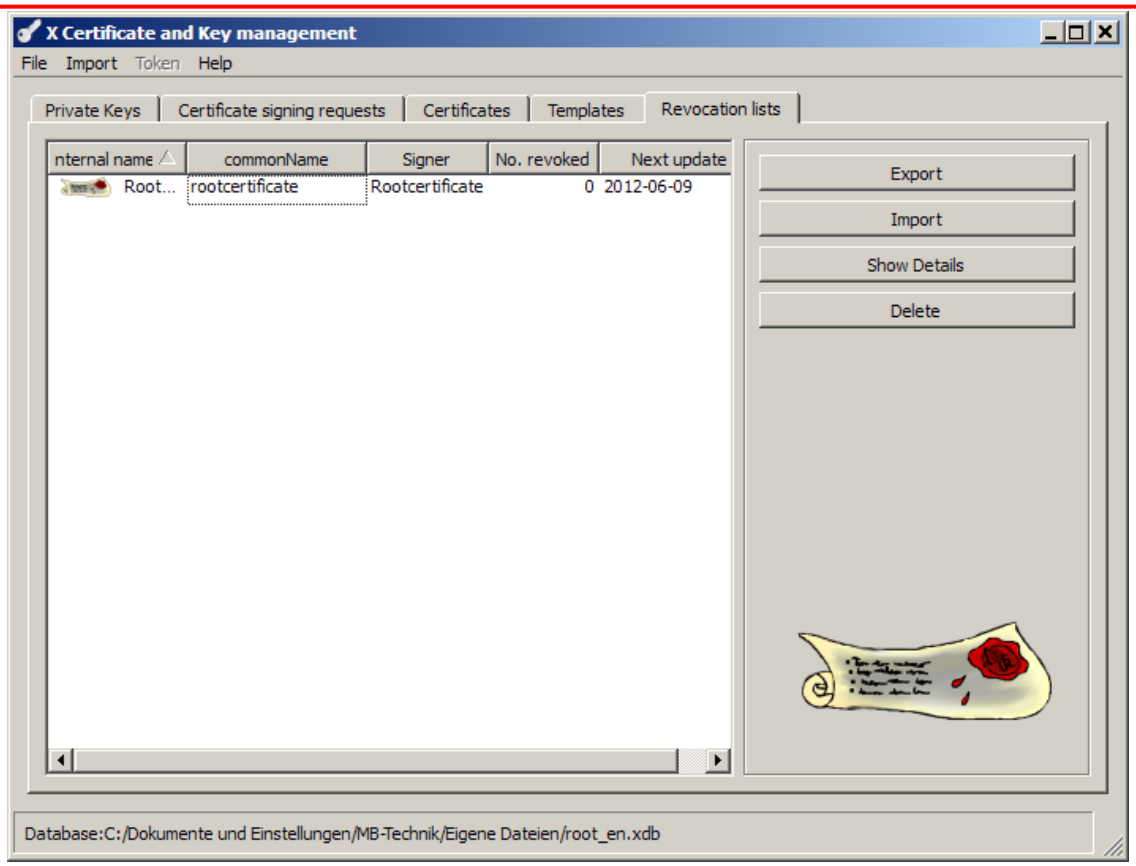


Figure 115

In the *"Revocation lists"* tab you now see the revocation list that you just created. Highlight it, and click *"Export"*. Select **.pem** as the export format. Choose a suitable save location, then confirm with OK. You can now import the list using the **System → Certificates** menu on the mbNET web interface (cf. section CRL). Restarting the VPN connection or the mbNET will enable the CRL and it will no longer be possible to establish a VPN tunnel using the revoked certificate.

11. Importing certificates in Windows XP

To import finished certificates, you need to set up what is known as a Certificate Management Console. To do this, click *"Start" -> "Run"* and type in "***MMC***". Then click on *"File – Add/Remove Snap-in"* and in the next screen, select *"Add"*. You can then select **Certificates** from the list of available snap-ins.

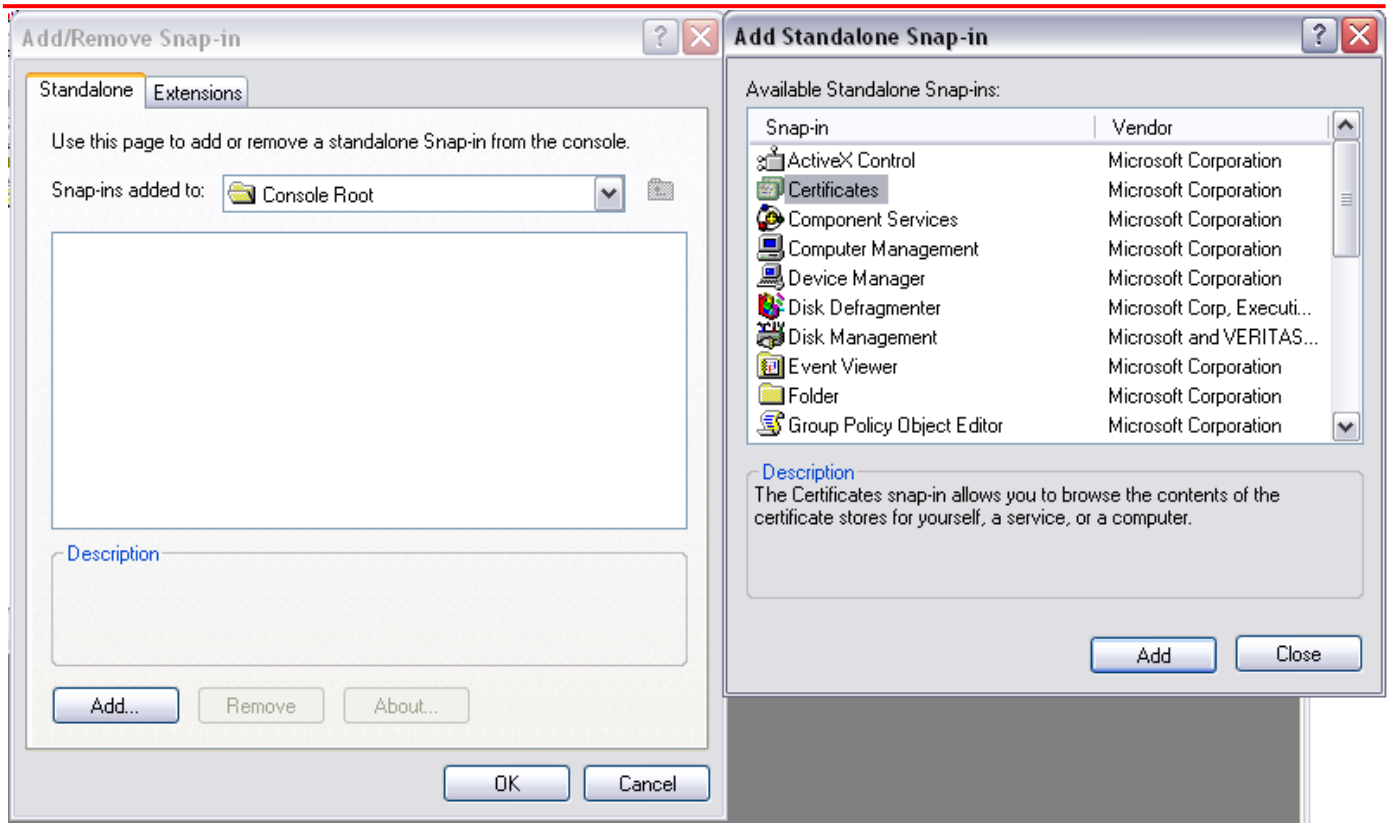


Figure 116

In the next window, select "*Computer account*":

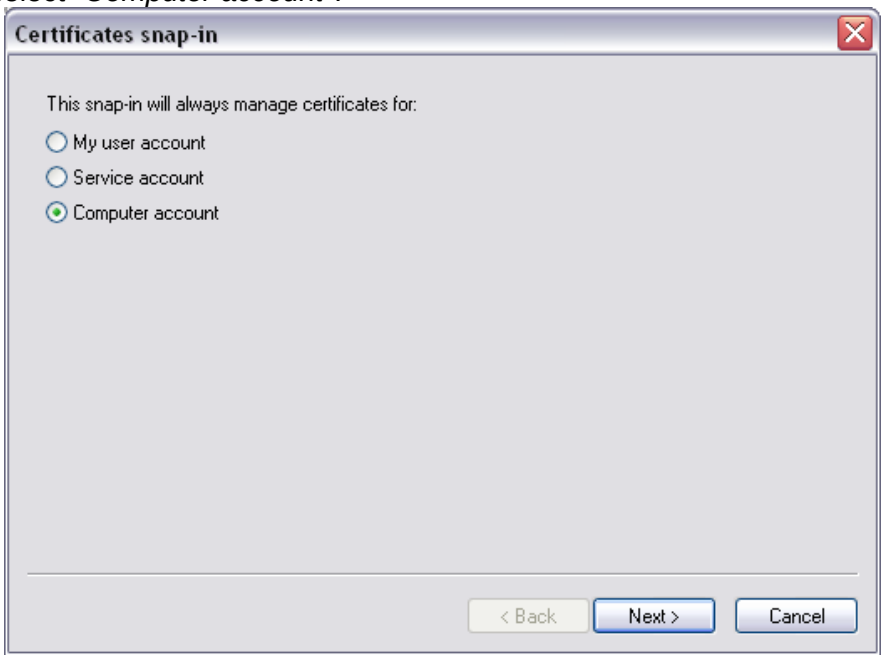


Figure 117

In the next screen, ensure that you select *"This Snap-in will always manage" ... "Local computer (computer running this console)*.
Once you have created the certificate console as described, you can **import a certificate**.

First, open the folder and right-click on *"Personal -> Certificates"* as shown in the screenshot below, and import the certificate that will be used to identify the client. Be sure to select the **".p12" file** for this. Enter the password for the p12 file and then click Next. In the next screen, select *"Automatically select the certificate store based on the type of certificate"*. When you click *"Finish"* the relevant certificates will import.

No further certificate imports are required. The CA certificate is automatically imported. Nor is it necessary to save the console.

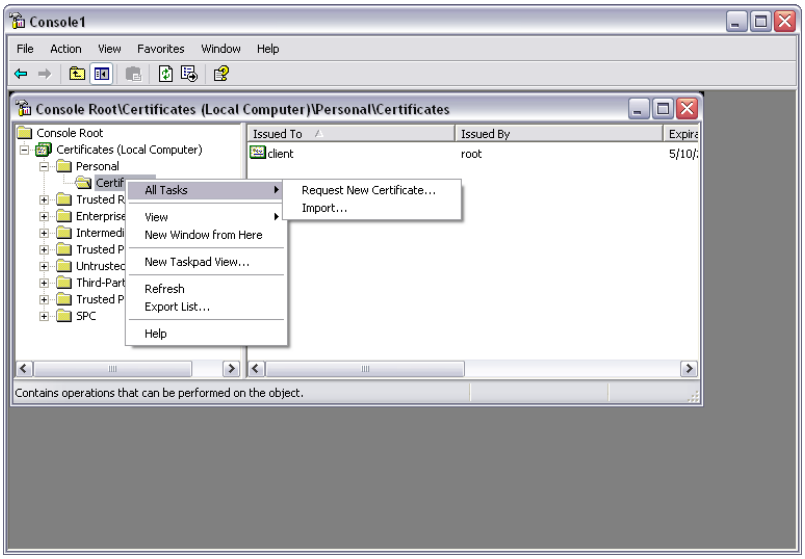


Figure 118

Double-clicking on the relevant certificate displays its properties. In the *"General"* tab you can check, amongst other things, which CA issued the certificate, how long it is valid for and whether you have a private key for it. This is very important when using certificates for web server publishing.

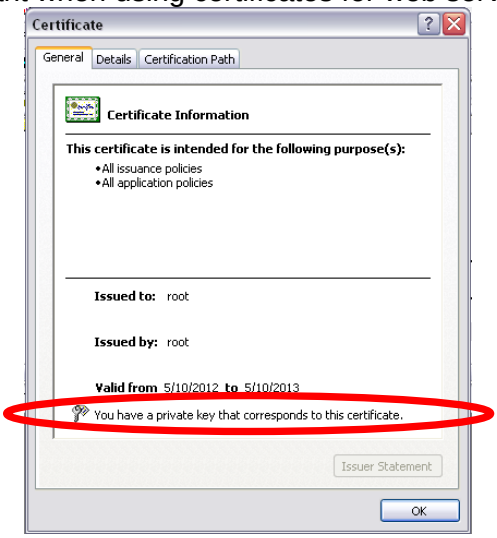


Figure 119

There is more information about the issued certificate in the *"Details"* tab.

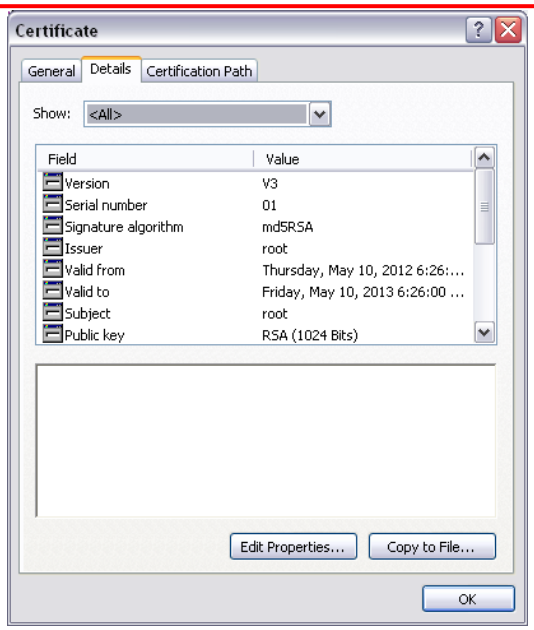


Figure 120

12. System Settings

The most important system settings have already been outlined above in **System Settings**. A more detailed explanation of additional system settings is given below.

12.1 System – WEB

Using HTTPS (Hypertext Transfer Protocol Secure; detects https: ***//...*** in the browser window) encrypts the connection between web browser and web server. Encryption is usually 40 or 128 Bit, depending on key size.

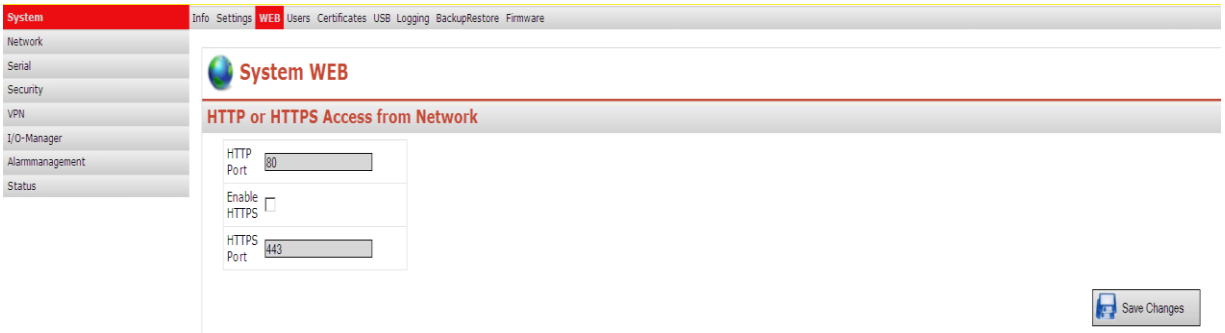


Figure 121

Label	Description
HTTP Port	The standard port for HTTP requests is TCP 80. You can change this if you need this port for your OpenVPN connection or if it is already being used for another purpose. If you do this however, note that you will need to enter the port in the browser along with the address. (Firmware versions 2.0.1 and higher)
Enable HTTPS	Clicking on the check box enables the secure Hypertext Transfer Protocol.
HTTPS Port	To allow remote station access, you need to enter the router IP address and the port. In this case: Port 443

12.2 System – Users

12.2.1 General

With user management you can:

- ❑ Give users access rights to web interface administration, and modem or VPN dial-in.
- ❑ Edit or delete existing users, or add new users.

12.2.2 Editing users

To edit a user, proceed as follows:

- ❑ Select **System** and then **Users**.
- ❑ To select a user whose rights you want to change, click on the **edit button**.
  The user will be displayed in the first row along with their access settings.

Figure 122

- ❑ Amend the relevant field entries and apply the changes.
- ❑ Save your changes by clicking Save (disk icon, figure 124)

Figure 123

- ❑ You can undo your changes by clicking on **Clear Changes**.

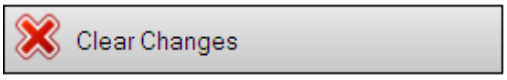


Figure 124

❑ Clicking on Apply Changes applies the changes to the router.

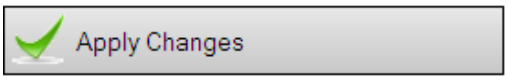


Figure 125

12.2.3 **Adding users**

To add a user, proceed as follows:

- In the navigation bar on the left, select **System** and then **Users**.

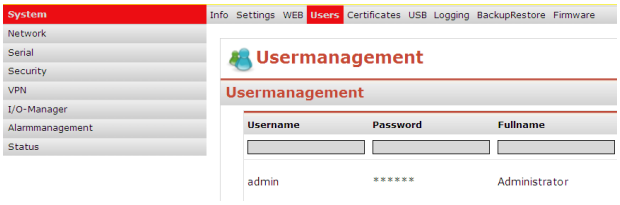


Figure 126

- In the first row of input fields, enter the **username**, **password** and **full name** of the user.

Please note:
all three fields must be completed otherwise you will receive an error message when you save.

❑ In the three check boxes that follow, specify which rights you want the new user to have. Choose whether the user

  - Can make settings in the web interface (Administration)
  - Can connect to the industrial router's modem (Modem dialin)
  - Can connect to the industrial router via VPN (VPN dialin)

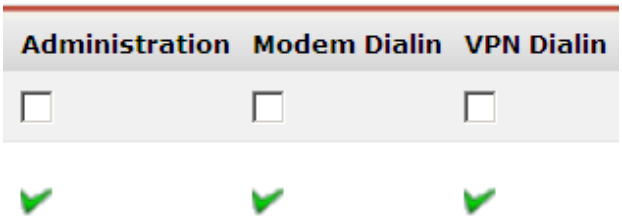


Figure 127

❑ Click the applicable **option box** to place a check in it.

Figure 128

- Click "Save Changes" to do a temporary save.

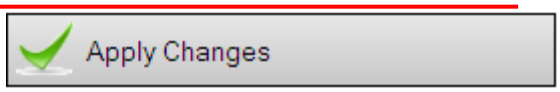


Figure 129

To apply the changes to the router, click **Apply Changes**

12.2.4 Deleting Users

To delete a user, proceed as follows:

- ❑ In the navigation bar on the left, select **System** and then **Users**
- ❑ Select the row that contains the user name, password and so on, and click the icon to **Delete**

Figure 130

To apply the settings to the router permanently, click **Apply Changes**

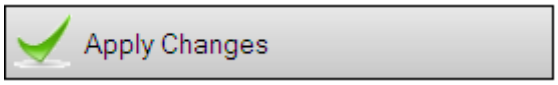


Figure 131

You will now no longer be able to log in or authenticate this user via the web interface, modem or VPN.

12.3 System – Certificates

A key component of VPN connections with IPSec or OpenVPN is the trust relationships between two or more communications peers. Authentication settings are made during configuration, as explained in the section **Authentication**.
For secure communication, authenticity needs to be verified. Certificates help to ensure also that the ***right*** peers are communicating with each other. A certificate is proof of the holder's identity. The certificate can be issued by a higher authority (called a Certificate Authority, CA for short) or by the actual certificate holder. The certificate holder is called the ***Subject***, and whoever issues the certificate is called the ***Issuer***.
Below is a screenshot of the relevant certificates tabs and the option to import a new certificate.

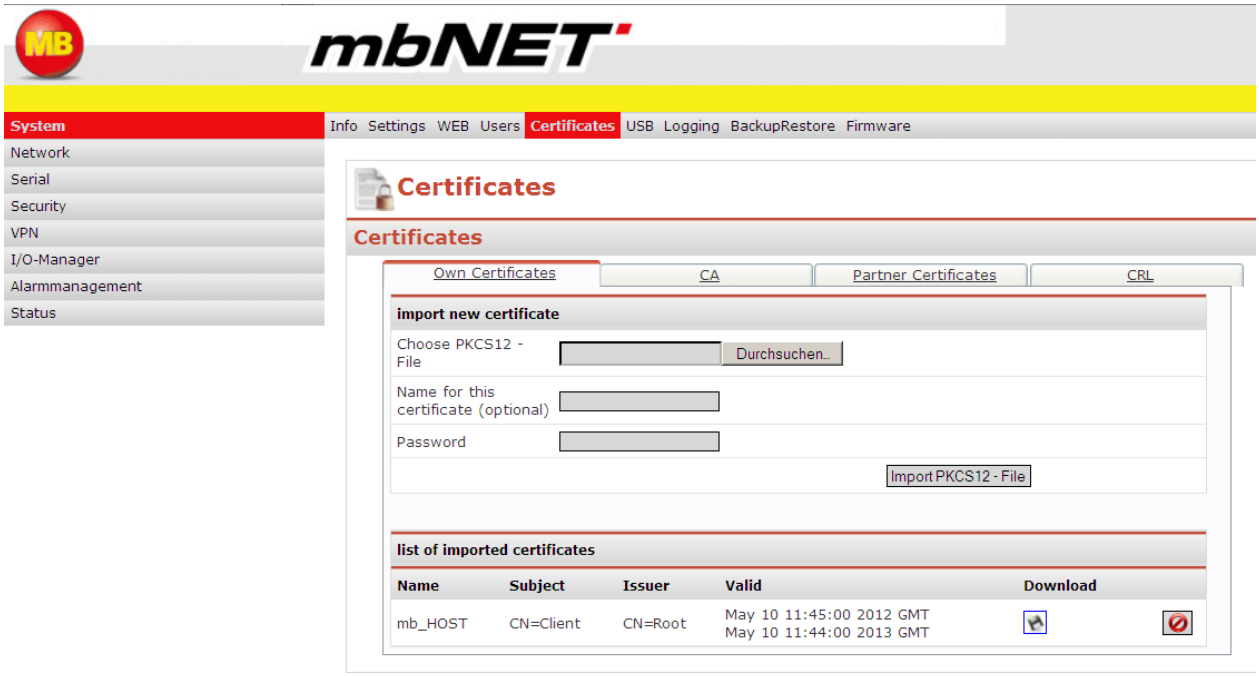


Figure 132

12.3.1 Personal Certificates

Personal certificates are used by the holder, but issued and signed by a higher-level authority (CA/root certificate). For the router to be able to show and use its personal certificate on a remote station, the relevant PKCS12 file (certificate plus private key) first has to be selected and imported to the router. Single or multiple PKCS files may be imported. Personal certificates also always have a key, which is why a PKCS12 file must be imported. This is actually made up of a .crt file and a .pem key file.

Please note that XCA bundles the key and the certificate to a single file with the extension ".p12". This is what is meant by a PKCS12 file.

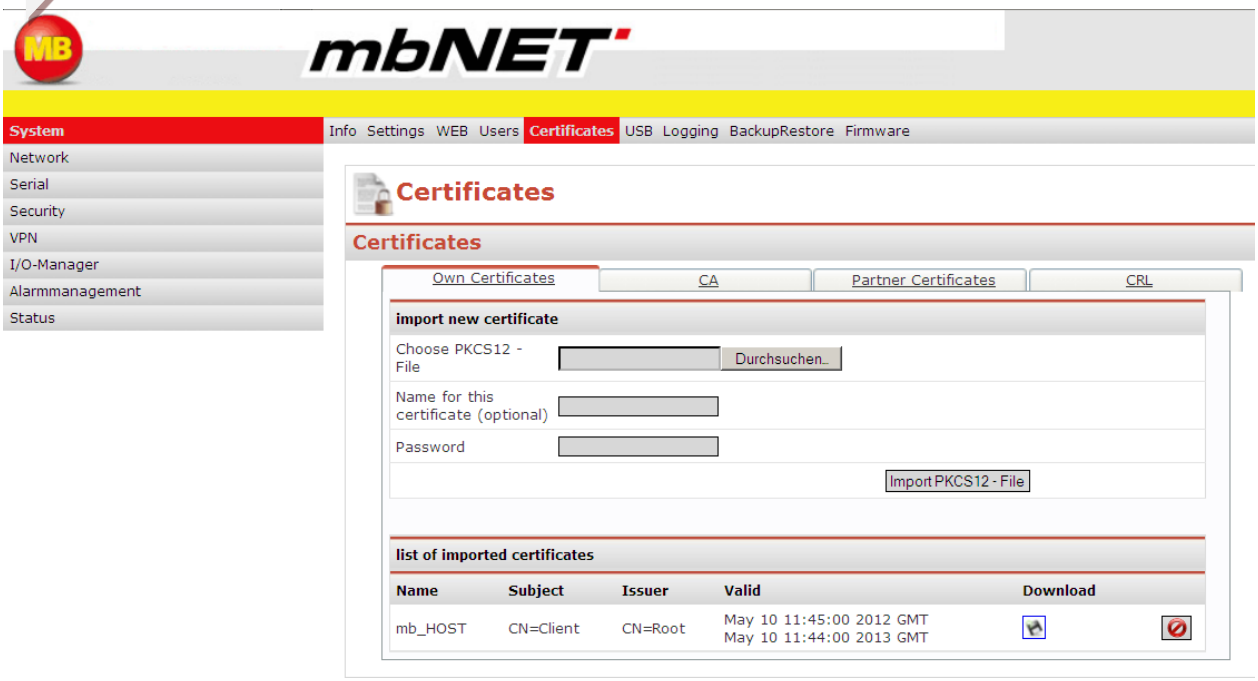


Figure 133

Label	Description			
Import new certificates	**Choose PKCS12 file:** certificate file selection (PKCS12 file). **Browse:** provides file path for certificate file. **Name for this certificate (optional):** optional entry of a name for the certificate file. **Password**: certificate password entry. The certificate must have been assigned a password when it was created, otherwise it will not import. **Import PKCS12 file:** As long as the above data have been entered correctly, clicking on this button imports the certificate.			
List of imported certificates	This displays a list of the certificates already imported. More certificates can be included by using **Import PKCS12 file**.			
Name	Name of the certificate: in this case, mb_HOST			
Subject (certificate holder)	Attributes of certificate holders – in the example, this is:			
	C		OU	
	ST		CN	Client
	L		emailAddress	
	O			

Label	Description	
Issuer	For an explanation, see **Subject (certificate holder)** on previous page.	
Valid	Shows how long the certificate is valid for.	
Download		There is a further step after clicking on this button: to download, right-click on the link and select **Save target as ....**.
		Clicking on this button allows you to reset or delete the list of imported certificates.

12.3.2 **Root certificate (CA)**

A root certificate verifies whether the remote station certificate is also signed by the root certificate. If the authentication method in the VPN settings is set to "Authentication by certificate from CA", this root certificate must then be imported. The entry in the root certificate is used to confirm that the person dialing in has a valid certificate. In other words, the CA certificate holds information on the validity of the certificate.
The CA certificate is available as a (CRT) file and needs to be imported to the router.

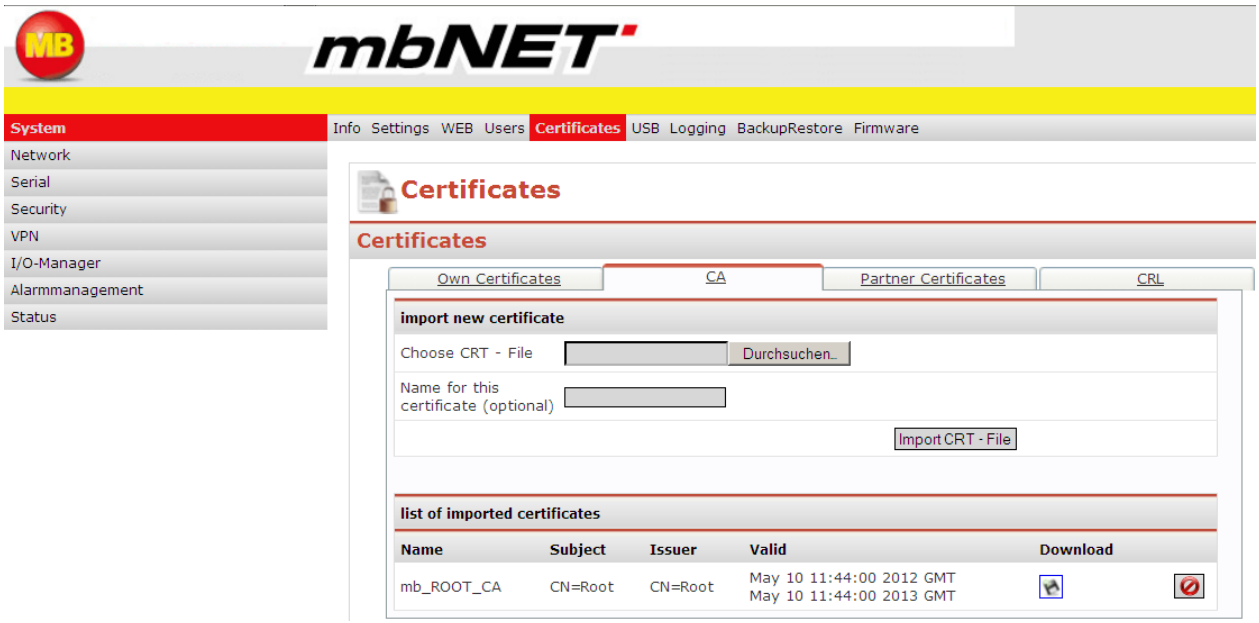


Figure 134

Label	Description

Import new certificates	**Choose CRT file:** enter the file location or browse the relevant drive for the certificate file. (File extension: .crt) **Name for this certificate (optional):** optional entry of a name for the certificate file. If you do not enter a name, the common name will be used **Import CRT file:** As long as the above data have been entered correctly, clicking on this button imports the certificate file.
List of imported certificates	This displays a list of the certificates already imported. More certificates can be collected by clicking **Import CRT File**. For more info on ***Name***, ***Subject***, ***Issuer***, ***Valid from/to*** and ***Download*** please see section **Personal Certificates**

12.3.3 Peer certificates (IPSec)

Peer certificates are remote station certificates. They are only needed if "Authentication by peer certificate" is selected in the VPN settings. In this situation the existence of a local copy of the certificate is confirmation of its validity.
The remote station certificate is selected via the relevant crt file and then imported. You can also import multiple crt files.

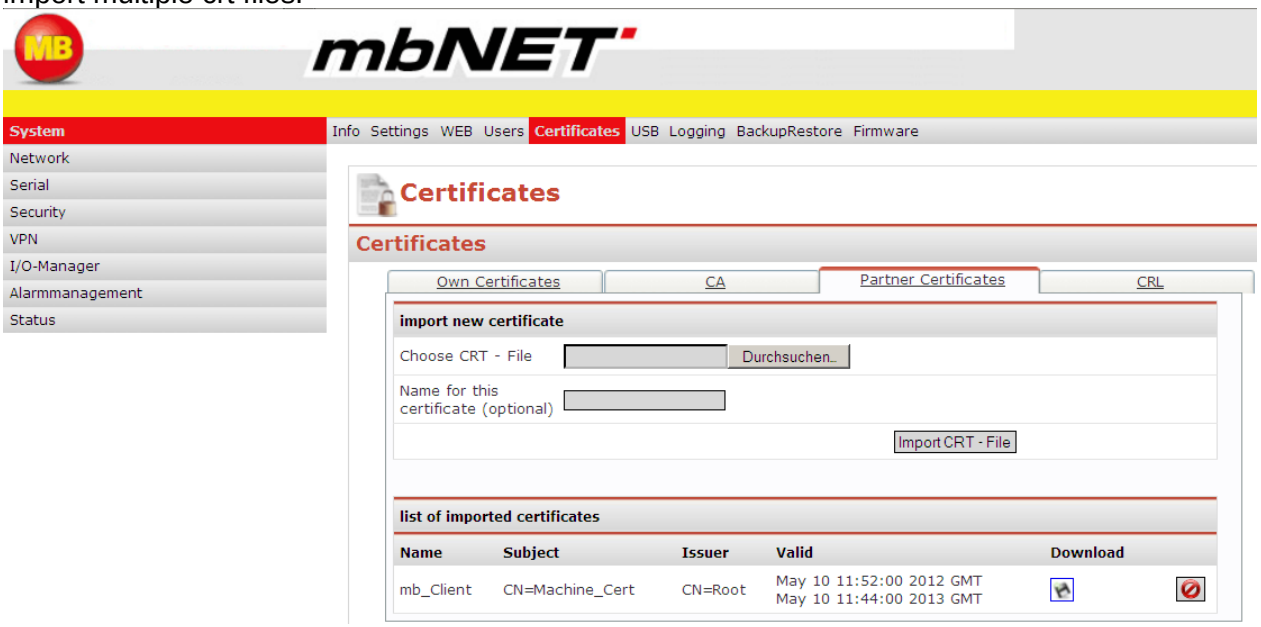


Figure 135

Label	Description
Import new certificates	**Choose CRT file:** enter the file location or browse the relevant drive for the certificate file. (File extension: .crt) **Name for this certificate (optional):** optional entry of a name for the certificate file. **Import CRT file:** as long as the above data have been entered correctly, the certificate file can be imported.
List of imported certificates	This displays a list of the certificates already imported. More certificate files can be collected by using **Import CRT file**. For more information on ***Name***, ***Subject***, ***Issuer***, ***valid from/to*** and ***Download*** please see section **Personal Certificates**

12.3.4 CRL

The Certificate Revocation List (CRL) is used to verify whether or not the computers dialing in hold valid certificates.
The CRL contains the serial numbers of certificates that should be blocked. So if you wish to withdraw someone's dial-in access rights to the router or the PLC behind it, you just need to create a CRL. XCA makes this easy.

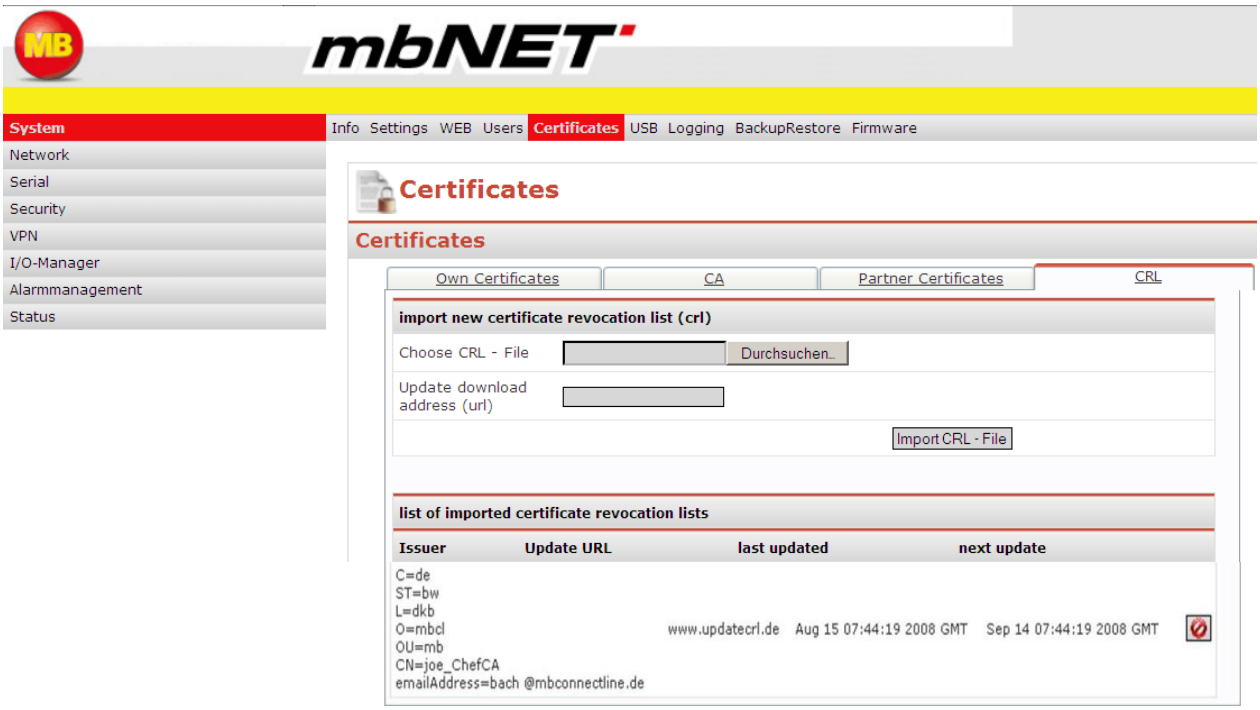


Figure 136

Label	Description
Importing new certificates	**Choose CRL File:** enter the file location or browse the relevant drive for the blacklist file. (File extension: .pem) **Update download address (url):** the PEM file can be regularly updated by entering the download address. **Import CRL file:** as long as the above data have been entered correctly, the blacklist file can be imported.
List of imported certificate revocation lists	This displays a list of the certificates already imported. More certificate files can be collected by using **Import CRL file**. For more information on ***Name***, ***Subject***, ***Issuer***, ***valid from/to*** and ***Download*** please see section **Personal Certificates**
Issuer	See section **Personal Certificates**
Update URL	Displays the update address for the blacklist file.
Last updated	Displays the date of the most recent update.
Next update	Displays the date of the next scheduled blacklist update.

12.4 System – USB

You can connect a USB device (flash or external drive) to the industrial router's USB port and make this available to network users as an additional drive.
To set up the USB port, select **System** on the navigation bar on the left and **USB** on the navigation bar at the top. This will display the screen shown below.

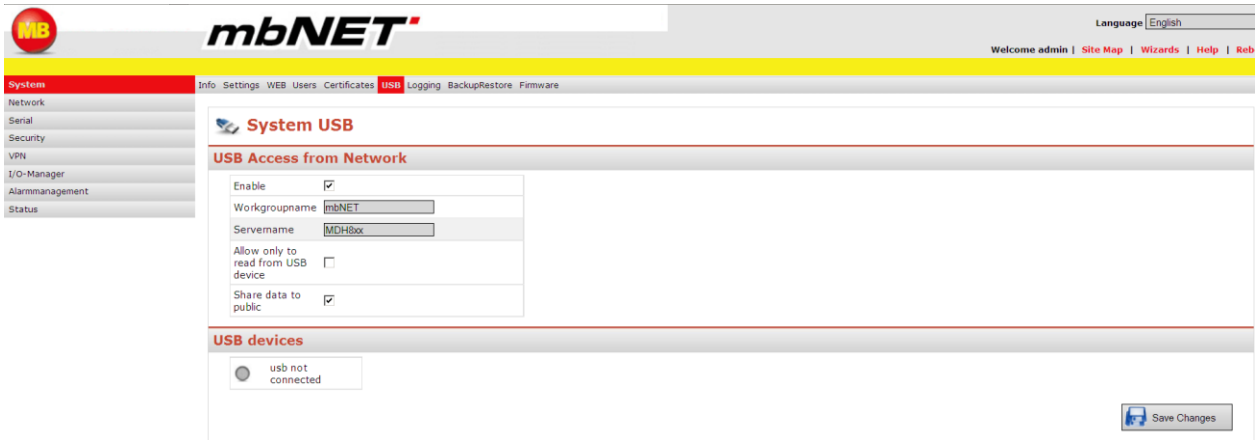


Figure 137

Label	Description
Enable	Select whether to enable connection of a USB device with the industrial router.
Workgroup-name	Enter the name of the workgroup through which users can access the drive.
Servername	Enter a name under which the USB drive will appear in the above mentioned workgroup.
Allow only to read from USB device	Select whether users will have read-only access to the USB drive, or can also save data to it.
Share data to public	Specify whether to give access rights to network users who are not registered under the industrial router's user management system.
USB devices	The bottom area of the screenshot shows whether a USB is connected. A connected USB device is indicated by a green dot.

Please note that the drive must have a FAT/FAT32 file system. Other file systems, e.g. NFTS, can cause problems.

12.5 System – Logging

System logging for the *mbNET* can be outsourced to another computer by using a log server.

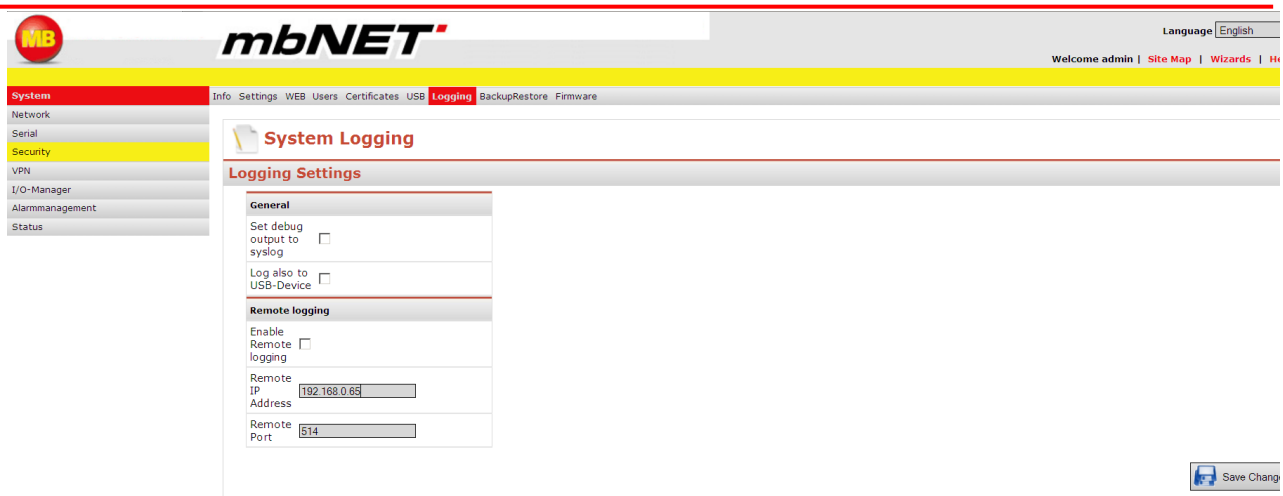


Figure 138

Label	Description
Enable Remote Logging	To enable a log server, place a check in the box by clicking on it. System logging for the *mbNET* industrial router can now be outsourced to another computer.
Remote IP Address	Remote IP address of log server. In this case: 192.168.0.65
Remote Port	Remote port for log server. In this case: Port 514 We recommend that you do not change this port, as certain applications may not work properly on a completely different port.

12.6 System – Configuration

Using this menu, you can both back up and restore a system configuration.
The configuration can be saved e.g. to a connected USB drive before making major changes, and if necessary, restored onto the industrial router.

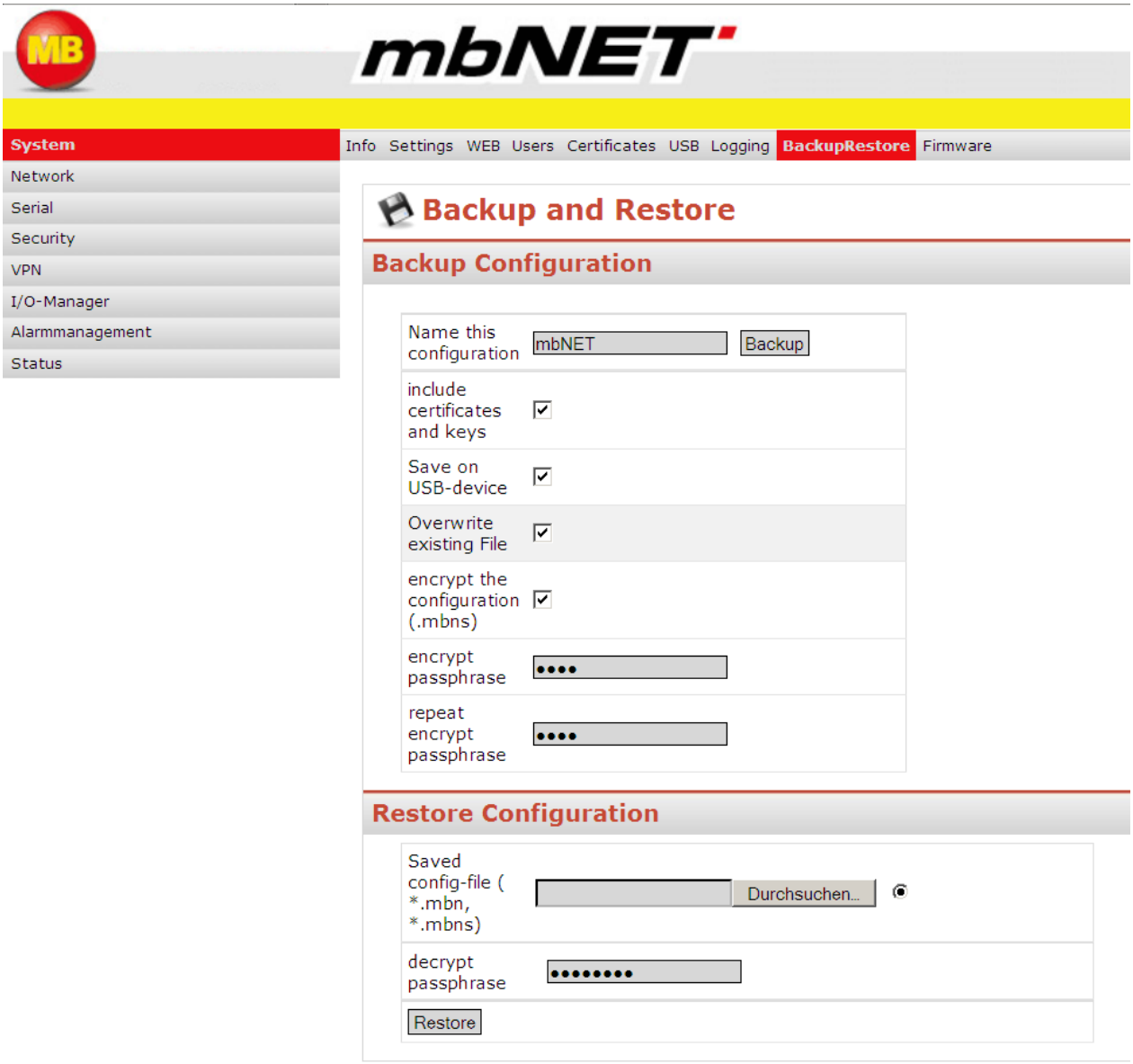


Figure 139

Label	Description
Name this configuration	Assign a meaningful name to the configuration. In this case: *mbNET*
Backup	Backs up the configuration. After clicking on this button you will be prompted to enter a location, e.g. the USB drive letter.
Include certificates and keys	This configures the system to copy an mbNET. Please note that this configuration file should only be used for one device.
Save on USB device	If a USB storage medium is connected, the configuration can also be stored there.
Overwrite existing file	If this option is not enabled, and a configuration file already exists at the same location, the new configuration will not be stored. Either change the name of one of the files, or choose a different save location for the new configuration.

Saved config file (*.mbn, .*mbns):	To restore a configuration, the stored file containing the router configuration must be restored, i.e. transferred back on to the industrial router. To perform a restore, first click **Browse**, then browse to the file location or directory and select the file. Then click on the **Restore** button.
Loading a configuration from a USB device	If the storage medium connected to the mbNET contains a configuration file, the file(s) will be displayed as in the example above. You can then select one of the files and click on **Restore**. You will be asked which areas of the configuration you would like to restore. Enable the areas that you want, and confirm. Finally you will be asked to restart the device.

12.7 System – Firmware

There are two ways to update the industrial router's firmware and these are explained below.

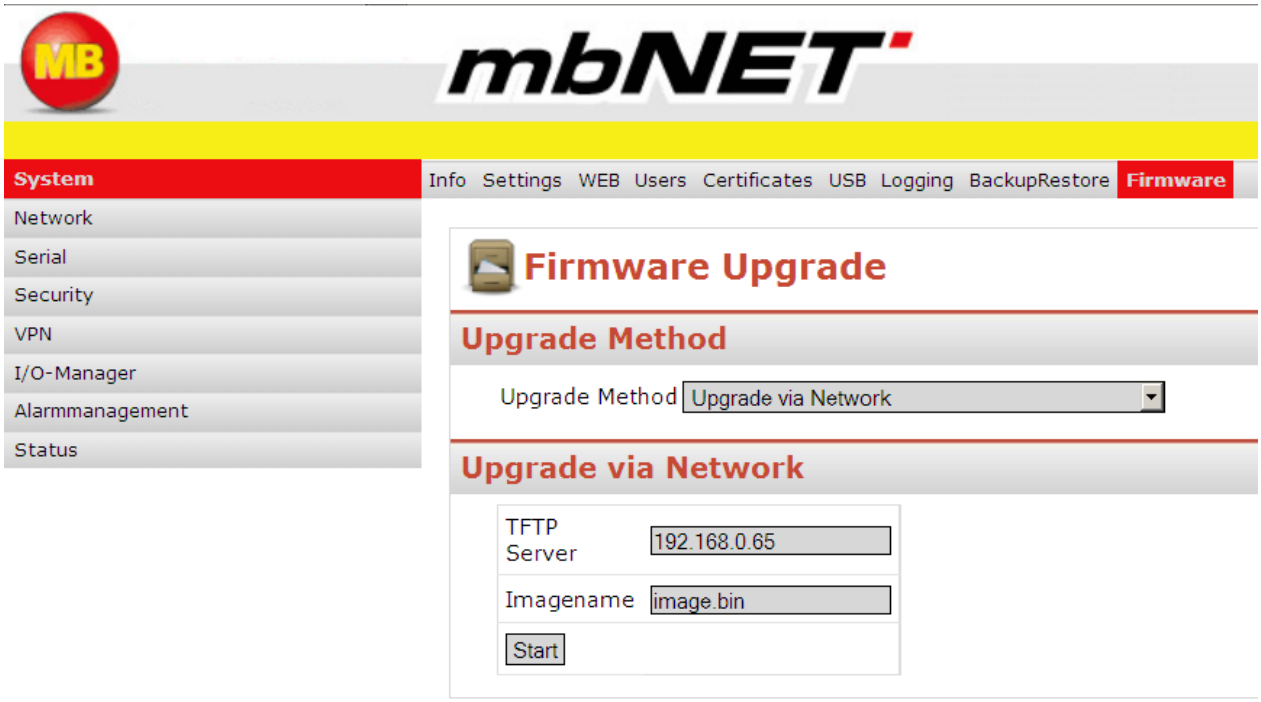


Figure 140

Label	Description
Upgrade method	When you click on the drop-down field, there are two options available for a firmware update: **Upgrade via USB:** This requires a USB storage device to be connected to the industrial router so that the file can be transferred across. The firmware name (image.bin) is listed here. To upgrade the firmware, click **Start**. Then restart the device. **Upgrade via Network:** In this case you need to enter the IP address of a TFTP server, and the firmware name. In this case: image.bin Before the upgrade can start, the "tftpd32" tool must be launched. You can download this free of charge at http://tftpd32.jounin.net/ . Once you launch the tool, enter the following settings in the "DHCP server" tab: IP poolstartingaddress: *IP address of the router that you are upgrading.* Size of pool: *10* Mask: *Network subnet mask*

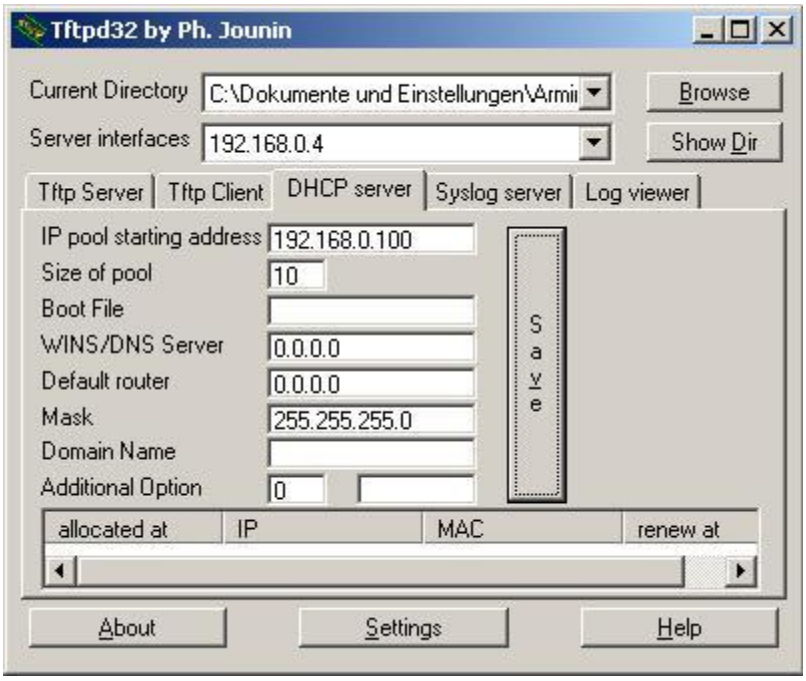


Figure 141

Clicking on **Save** will store the settings. In the drop-down field under "Current Directory", you need to select the folder where the firmware upgrade file is saved. Do not close the tool until the upgrade is complete. Now, in the web interface TFTP Server field, you need to enter the IP of the computer that is currently running Tftpd32. Now click **Start**. Once the process is complete, restart the device.

NEVER INTERRUPT THE MBNET DURING A FIRMWARE UPGRADE! If you do, the device will no longer be able to start.

13. Network

13.1 Network – LAN

LAN configuration allows you to configure the router IP address (LAN address) and subnet mask. This is the IP address used for accessing the router from the LAN.

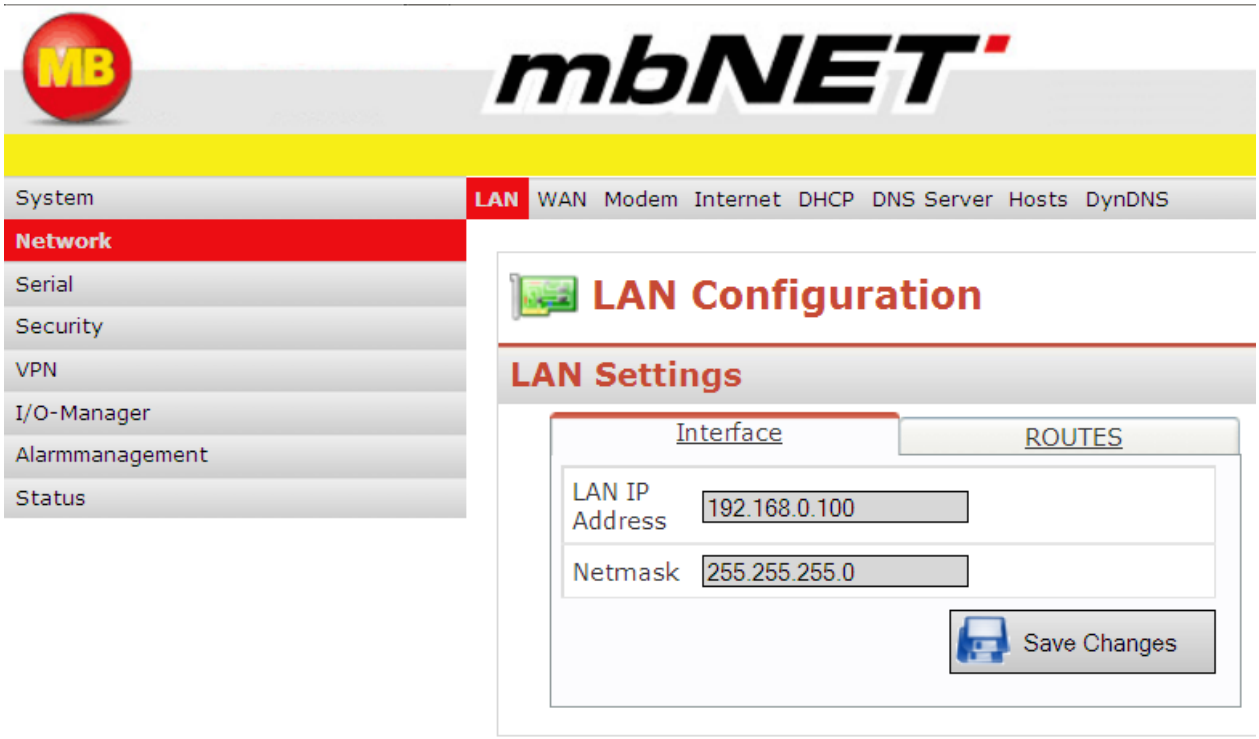


Figure 142

Label	Description
Interface	To set up the LAN interface, click on the tab.
LAN IP address	Enter the router IP address.
Netmask	Enter the subnet mask of the network into which the router is to be integrated.
Routes	To set up specific routes, click on the Routes tab. You can enter both network routes in CIDR format (x.x.x.0/24) and host routes here.

13.2 Network – WAN

The industrial router's WAN interface can connect a local network with a remote network, or with a public network like the Internet. Therefore the WAN interface is configured according to how it will be used.

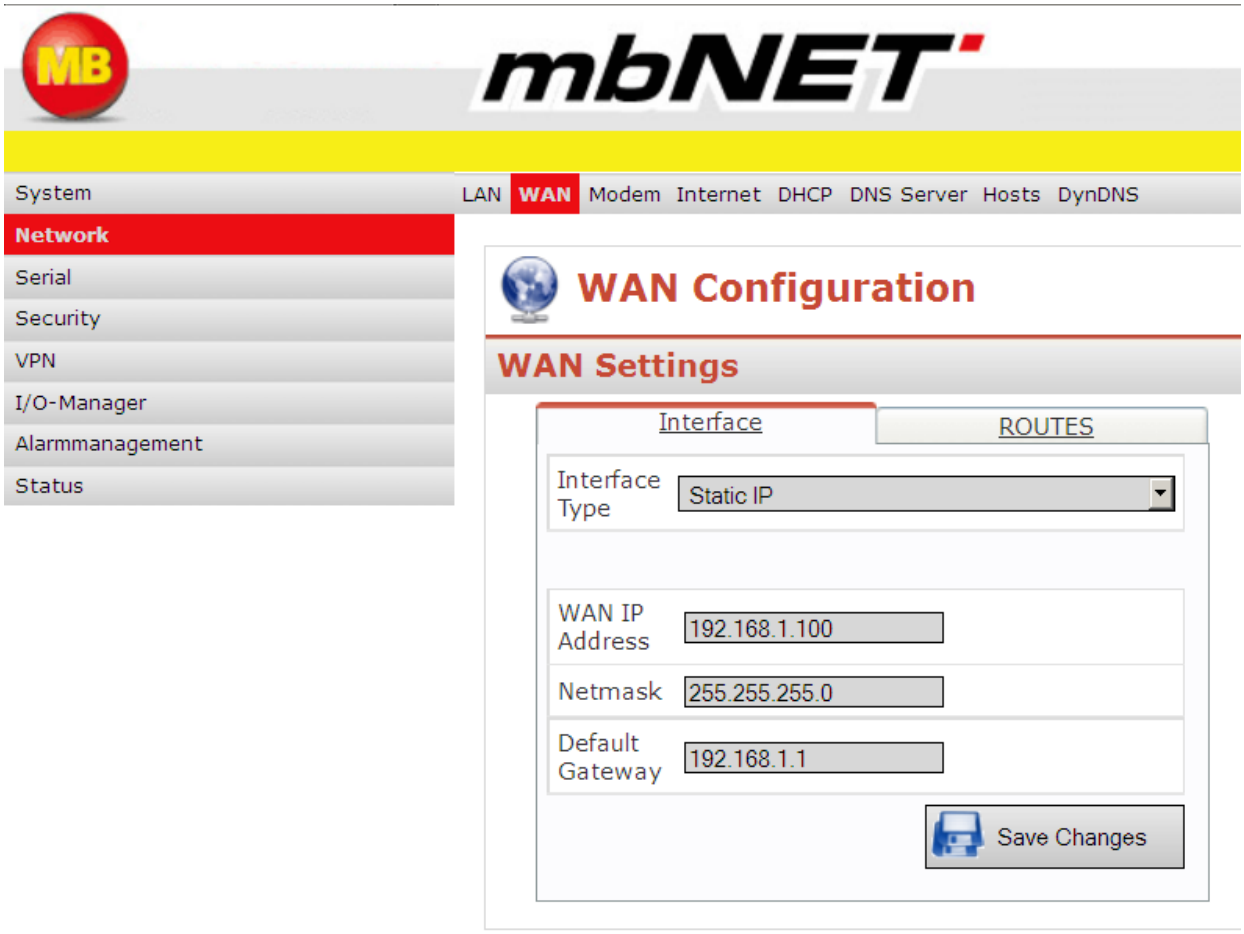


Figure 143

Label	Description
Interface Type	You can select from the following interface types: **DSL:** select this option if your router is directly connected to a DSL modem that connects to the Internet. **DHCP:** select this setting if there is a DHCP server on the network which is therefore automatically assigned a new IP address by the industrial router. **Please also contact your network administrator to confirm this.** **Static IP:** select this setting if connection to the Internet is via an existing router which is not acting as a DHCP sever, or if no server is set up to assign addresses. You should also select this setting if you have received a static address from your ISP, e.g. if you have a leased line. Note also that this type of connection requires you to enter a DNS server (see **Network – DNS Server**). **WAN IP address:** IP address of the router connected to the WAN port. **Netmask:** enter the subnet mask. **Default gateway:** enter details of the gateway that connects you to the Internet, i.e. the IP address of the existing router.

13.3 Network – Modem

13.3.1 Network – Modem – Incoming

Network – WAN (continued)

Label	Description
Connection mode	**When selecting interface type, choosing DSL also requires you to select one of the following options:** **PPPoE:** Select this option if your ISP requires a PPPoE (Point to Point Protocol over Ethernet) connection. A lot of modems are set to this option. The external IP address that a remote station uses to access the router is specified by the ISP. Please refer to your ISP documentation for the necessary details. **PPP User Login:** enter your Internet access user name as provided by your ISP. **PPP User Pass:** Enter your Internet access password as provided by your ISP. **PPTP:** Select this option if your ISP requires a PPTP connection (Point to Point Tunneling Protocol) connection. For example, in Austria, PPTP is used with DSL connections. **PPP User Login:** see the access user name provided by your ISP. **PPP User Pass:** see the access password provided by your ISP. **WAN IP address:** here, enter the IP address of the *mbNET* router connected to the WAN port. This is the address that devices use to access the router if they are connected to the **WAN**. If your ISP's IP address is not automatically assigned here, you should manually enter the IP that the PPTP server uses to access the router. Please refer to your ISP documentation for the necessary details. **Subnet mask:** enter the subnet mask of the network connected to the LAN port. **PPTP Server IP address:** enter your ISP server IP address.
Routes	This enables you to specify routes to other networks. If the local network has additional subnetworks, you can specify routes for these here. You can enter network routes in CIDR format (x.x.x.0/24) or routes to individual subscribers here.

The industrial router's integrated modem is for dial-in or Internet connection (analog, ISDN, GSM) where there is no available DSL or network connection.

NOTE:
If the modem is used for an outgoing Internet connection, it cannot be used for an incoming connection.

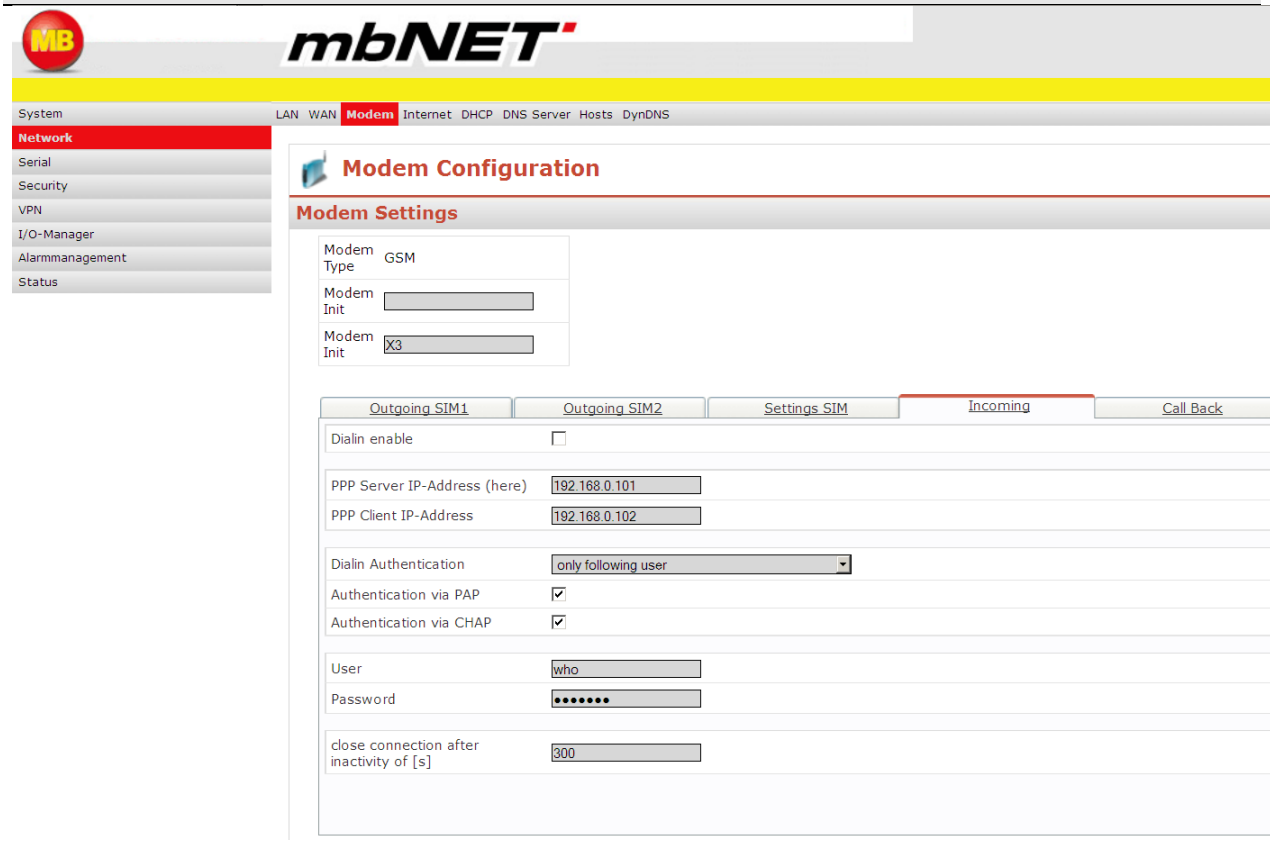


Figure 144

Label	Description
Modem Init	**ANALOG:** If using an analog device, enter the command **+GCI=country code** (for country codes, see **Country codes for analog devices**) here, and in the second row, the command **X3** (do not wait for dial tone). **ISDN:** If using an ISDN device, you need to enter your MSN number with the command **AT#Z=n** (n= MSN number) If you enter "n" as "*", every call will be accepted. **GSM:** if using a GSM device, you must use the preset X3 command. The **+GCI=country code** may not be used.

Label	Description
Incoming	You need to enable this option for the router to handle incoming dial-in or ISDN connections.
Dial-in enable	You need to enable this function by checking the box so that a client computer can access the router.
PPP Server IP-Address (here)	You need to enter the router IP address here. You can use the same network area as the local network. But please ensure that you do not re-use assigned addresses as this may lead to address conflicts.

PPP Client IP-Address	Here, enter the IP address that the router sends to the client (the remote station dialing in) as soon as a PPP connection is established. On connection, the router and the remote station establish a separate network.
Dialin Authentication	Specify whether a user name and password (i.e. authentication) will be required to dial in to the router. The options are: ❑ only following user: only the user entered in subsequent input fields in this dialog window has rights to dial in to the router. ❑ every user with dialin rights: any user who has been assigned "modem" rights under user management can dial in.
Authentication via PAP / CHAP	Use the default setting. PAP/CHAP are types of authentication. Ensure that this setting matches that of the subscribers dialing in. Disabling PAP/CHAP means that this authentication will not be accepted and that your sent data can be read by others.
User name & password	Enter the user name and associated password for PPP dial-in. These fields will only be available if you selected "only following user".
Close connection after ... [s] inactivity	Here you need to enter the length of time before the existing connection is to be dropped if no data has been transferred in the interim. If you leave this blank, or enter "0", the connection will not be dropped.

13.3.2 **Network – Modem – Outgoing**

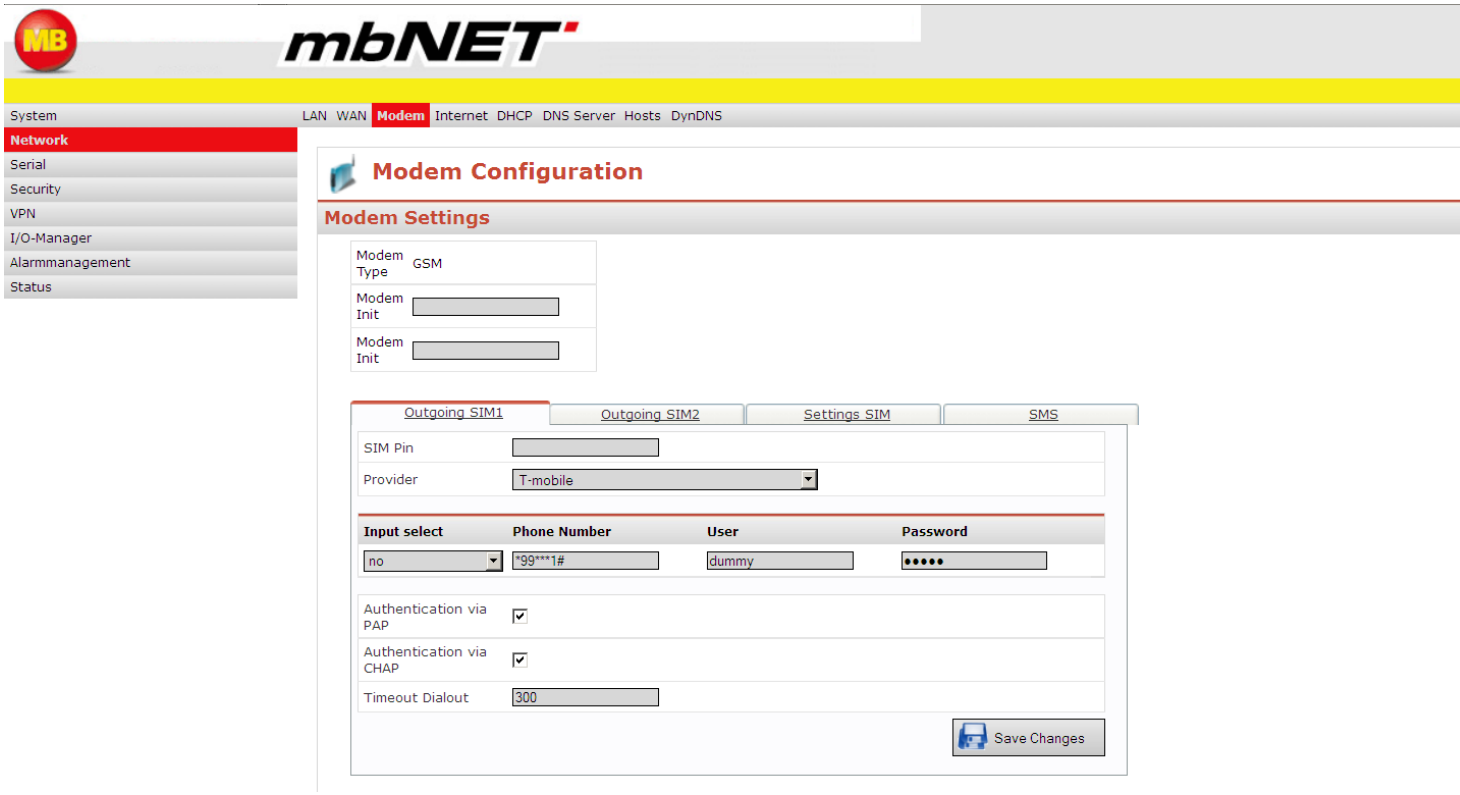


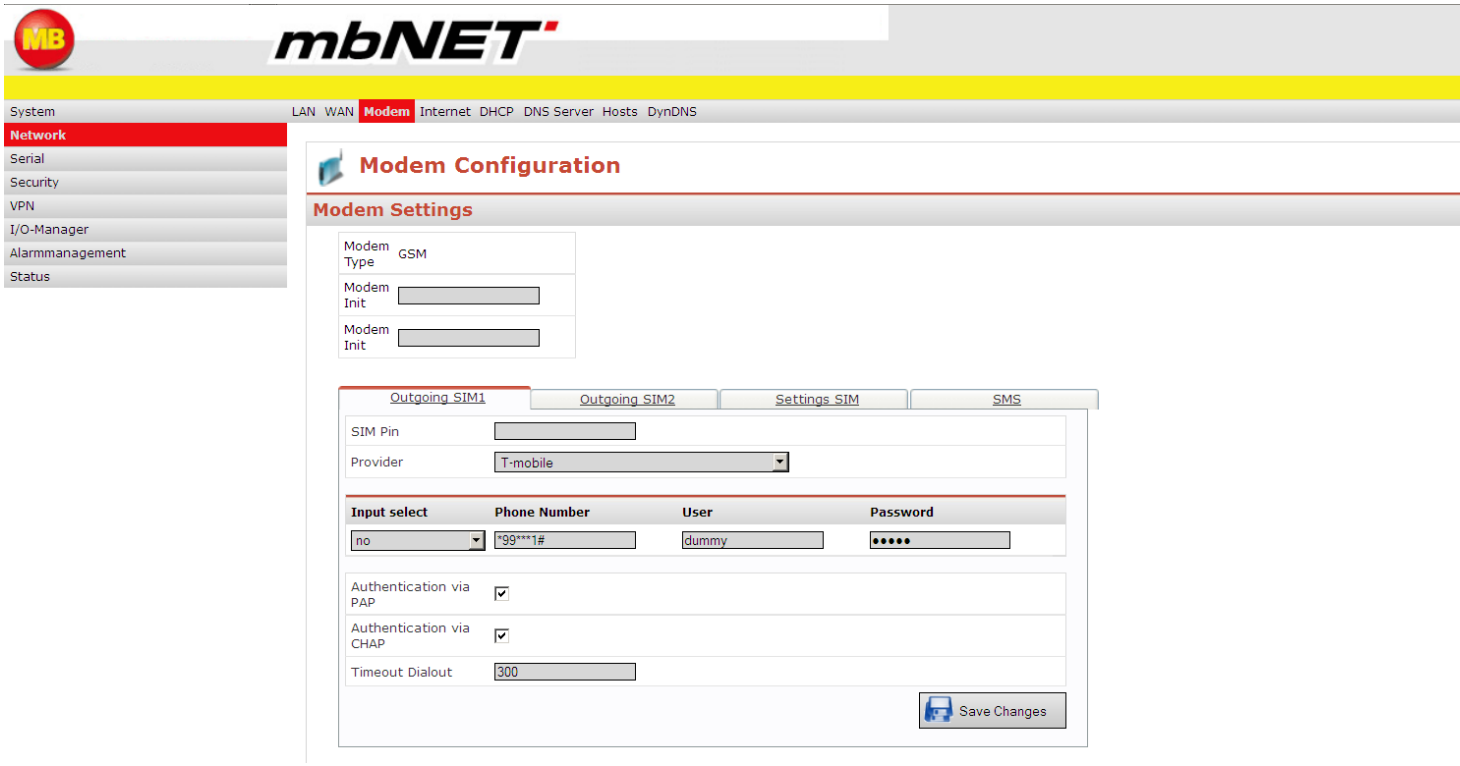
Figure 145

The following settings apply to outgoing modem connections

Label	Description
Input select	If you would like to call multiple terminals, set this option to "yes". You will then see three more fields where you can enter numbers that will be selected on receipt of a signal at digital inputs 2 to 4. Enter the numbers and user credentials for PPP dial-in in these additional fields. Switch on the first, and one or two of the other three inputs to start dialing. Note that you need to switch on the one/two other inputs before switching on the first. Also note that the industrial router is acting only as a PPP client here, and that there must be another industrial router, or a computer, acting as the PPP server to handle the request. Under Network – Internet, set the Internet connection to "On demand" and set the subsequent option to "Connect on Sign 1 at Input". • To call the first number: switch on input 1 • To call the second number: switch on input 2 and then input 1 • To call the third number: switch on input 3 and then input 1 • To call the fourth number: switch on input 2&3 and then input 1
Telephone number	Here, enter the telephone number of the relevant mobile broadband provider. For GSM modems this number always uses the format *99***1#

User	Enter the user name required to dial in via the relevant provider. You can obtain further details on this direct from your provider. For GSM modems there is more information for example at http://www.mbconnectline.de/gsm/grps/mobilfunk.html
Password	Enter the password required to dial in via the relevant provider. You can obtain further details on this direct from your provider. For GSM modems there is more information for example at http://www.mbconnectline.de/gsm/grps/mobilfunk.html
Authentication via PAP	Use the default setting for the authentication protocol. In principle this is preset when a dial-up connection is set up.
Authentication via CHAP	Use the default setting for the authentication protocol. In principle this is preset when a dial-up connection is set up. As a rule, CHAP is the process used by ISPs for Internet access log in via a modem or ISDN adapter.
Timeout dialout in [s]	After the length of time entered here, dialing attempts will stop, and restart anew.

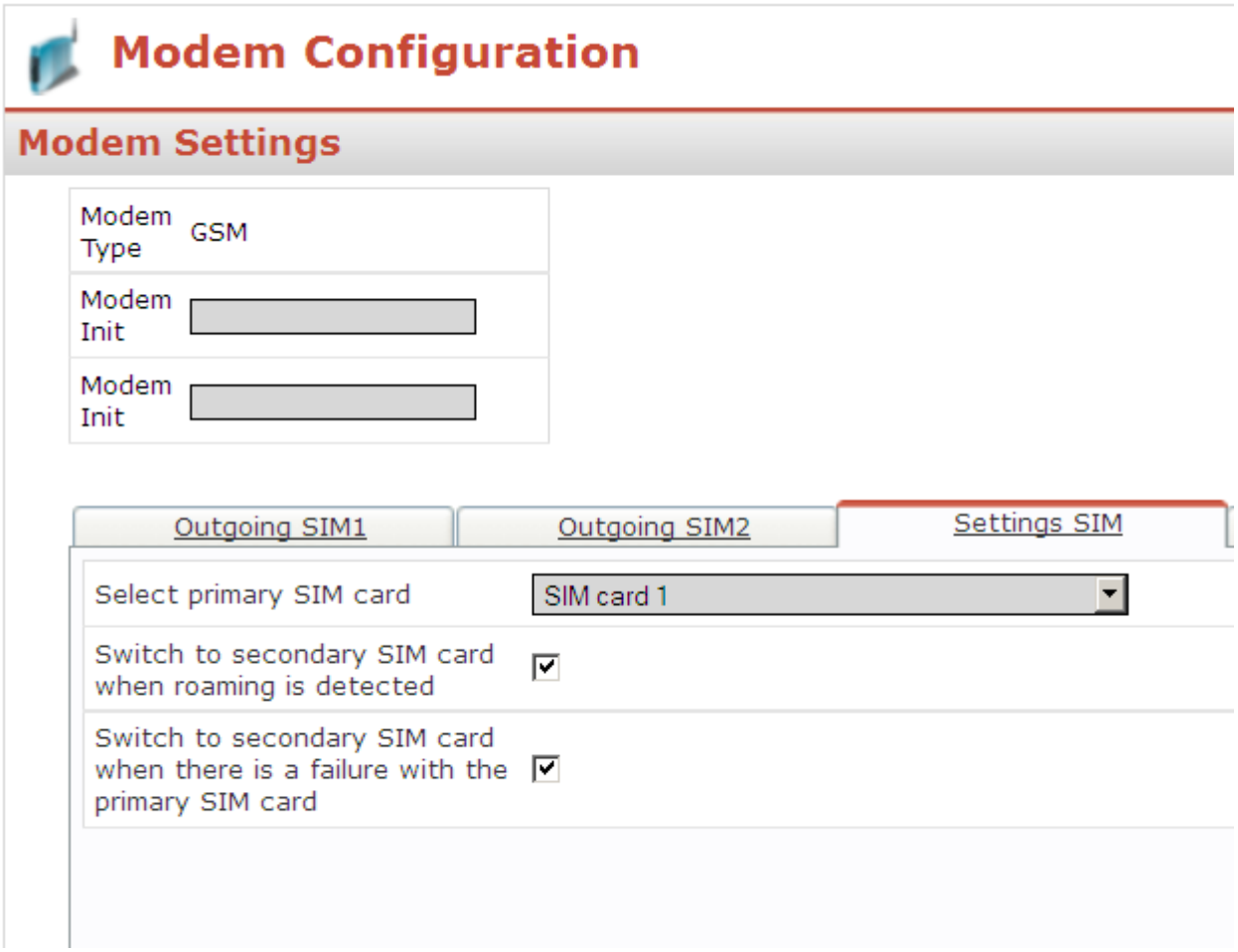
For MDH8xx mobile broadband devices there are two "Outgoing" menus. These are simply SIM1 and SIM2. There is also a second menu, "SMS" settings.



- The SIM cards can be from different providers
- SIM1 and SIM2 switch if there is a network fault, or while roaming.
- Remote control using SMS

Label	Description
SIM PIN	Enter the SIM card personal identification number (PIN) to ensure access. If you would like to switch PIN security on or off, you will need a cellphone
Provider	Select your mobile broadband network provider (e.g. T-mobile). If you want to enter an access point name (APN), select "Other". This opens a new window where you can enter the APN. For a list of APNs, go to http://www.mbconnectline.de/gsm/grps/mobilfunk.html. This takes you automatically to the relevant page on MB Connect Line's website.

13.3.3 SMS menu settings



First, we need to specify a primary SIM card, which will always be verified or used first. The secondary SIM card is always the non-primary one.
Switching is based on two (selectable) criteria:

- The SIM card fails to initialize, or to register on the cellphone network
- Roaming is detected on the SIM

13.3.4 Network – Modem – Callback

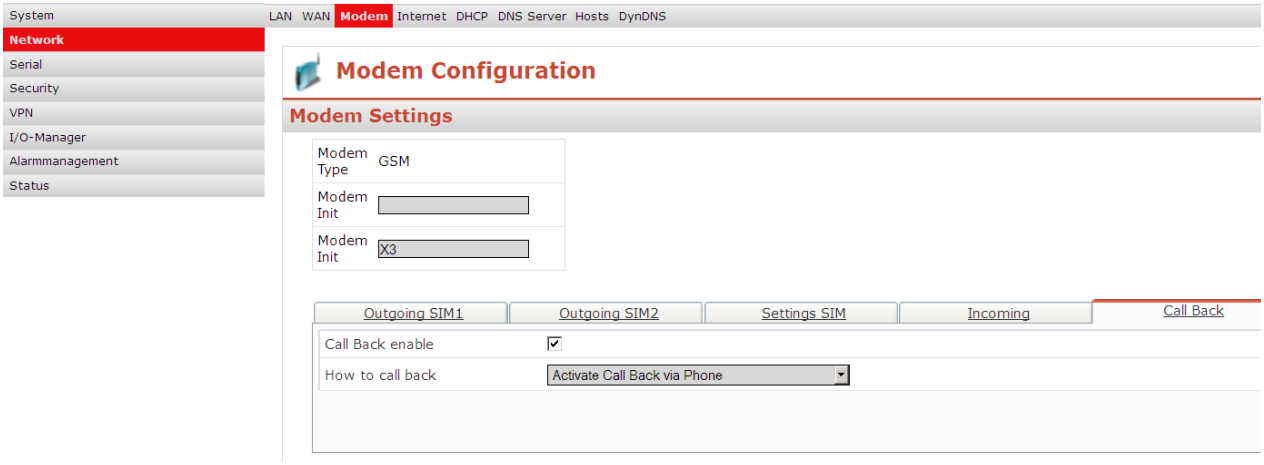


Figure 146

The settings below apply to the call back function. This function triggers Internet dial-in remotely via a telephone or dial-up connection. It must be set up so that the Internet connection will be established via WAN or modem. **Note that call back does NOT work with UMTS-enabled devices.**

Label	Description
Call back enable	Checking this option enables the call back function.
How to call back	**Activate Call Back via Phone:** With this setting, the *mbNET* will connect to the Internet if called from a phone. To establish a connection, the mbNET must be alerted by four rings. After this happens, the mbNET hangs up and then starts Internet dial-in. This can take 30-40 seconds. **Log in and press a button:** With this setting, the *mbNET* will connect to the Internet if you have set up a dial-up connection with the *mbNET* and you click on the Call Back button in the **System – Info** menu of the user interface. After 30 seconds, the *mbNET* will establish an Internet connection unless you close the dial-up connection.

13.3.5 Network – Modem – SMS

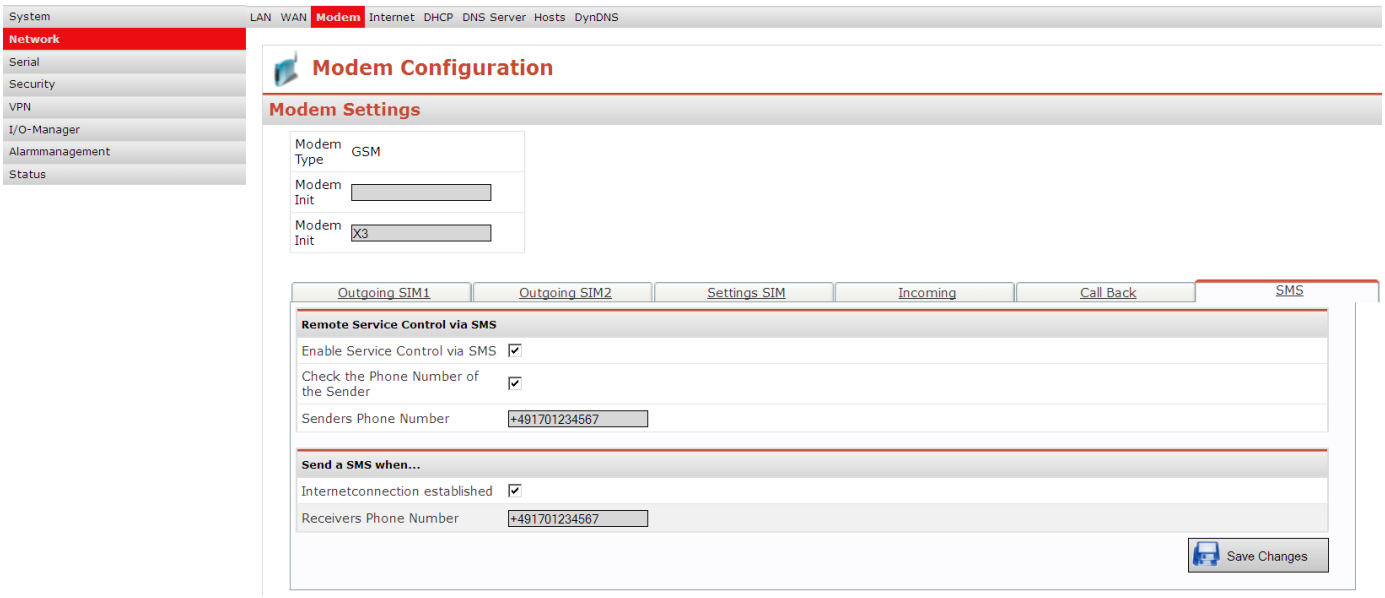


Figure 147

Label	Description
Enable Service Control via SMS	This function enables the use of service control via SMS
Check the Phone Number of the Sender	This ensures that the mbNET only accepts SMS commands from a specific number. Then enter the sender's cell number in "Senders Phone Number" in the next field. Commands sent from any other number will now be rejected.
Send an SMS when Internet Connection Established	The mbNET can send you an SMS as soon as it has connected to the Internet. In the next field, you also need to enter the telephone number to which this SMS should be sent.

Please note that your cell numbers cannot begin with 0. You must use the international format e.g. +49 for Germany.

13.3.6 Remote service control commands using SMS

- ***INET START*** or ***INET STOP***
  This controls the industrial router's Internet connection. Note that you can only control an Internet connection that is active and has been established by the industrial router.
- ***IPSEC START [connection name]*** or ***IPSEC STOP [connection name]***
  PPTP START [connection name] or ***PPTP STOP [connection name]***
  OPENVPN START [connection name] or ***OPENVPN STOP [connection name]***
  Whichever type of VPN you select, this must always be followed by the name of the connection (e.g. OPENVPN START Wizard). In addition, be aware that connection name is case sensitive.
- ***REBOOT***
  This will restart your industrial router. Please note that it cannot receive any commands while restarting.
- ***OUT ON*** or ***OUT OFF***
  Using ***OUT ON[outputnumber]*** or ***OUT OFF[outputnumber]*** you can also switch your

router's inputs on or off (e.g. OUT ON 1 switches on output 1; OUT OFF 1 switches off output 1)

- ***IN STATUS***
  The ***IN STATUS*** command returns input status
- ***GSM CMD***
  Using the ***GSM CMD [at-command]*** you can send any AT command to the modem. The modem response will be returned to the sender's number by SMS (e.g. "GSM CMD AT+cops?" returns network and provider details). Please note that only the first 160 characters of the modem response will be transmitted.

13.4 Network – Internet

Router Internet dial-in is dependent on connection type and on the appropriate configuration of specific settings.

13.4.1 Network – Internet – Internet Connections

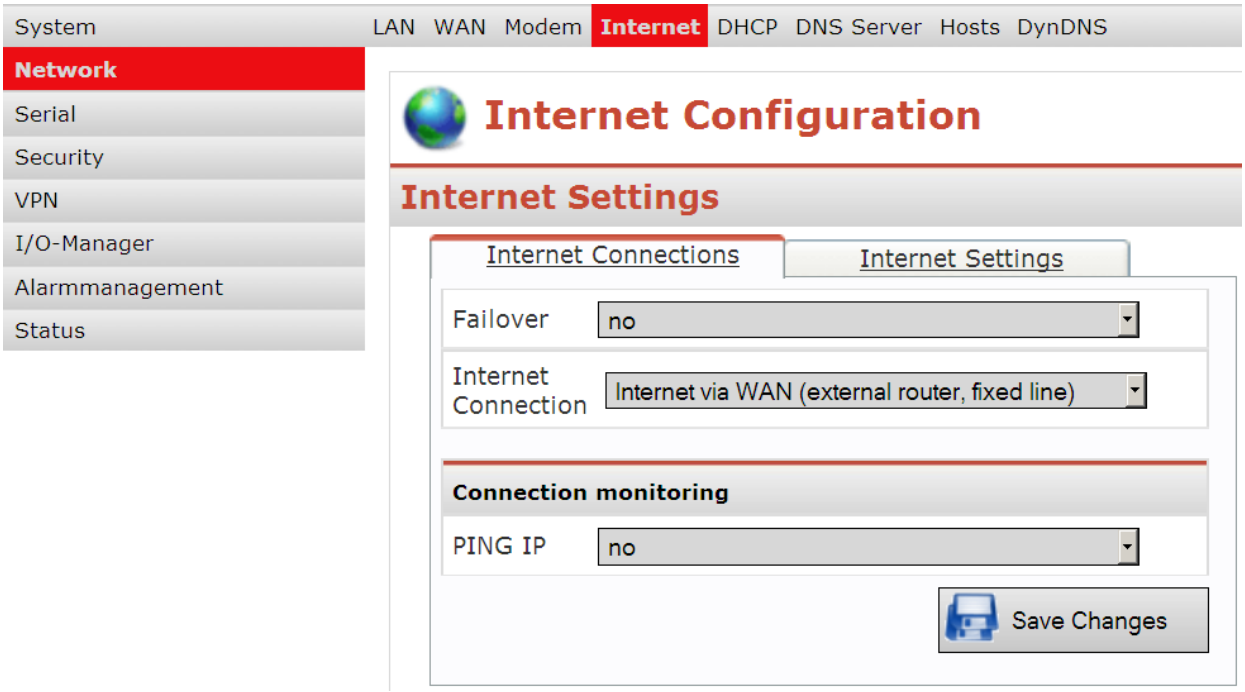


Figure 148

Label	Function
Failover enable	The failover function makes it possible to switch between different Internet connections. When this is enabled, you can set up a priority order for Internet interfaces, based on device model.
Internet connection	The following options are available from the drop-down field: ❑ **Internet via WAN (external router, fixed line)** Select this setting if the mbNET itself does not establish an Internet connection. This applies for example if your network has another router that is used for

	connecting to the Internet, or if there is only incoming dial-up via the public telephone network. ❑ **Internet via modem** Using this setting establishes a connection via modem. This requires access data to be entered in the settings under **Network – Modem**. ❑ **Internet via WAN** If you want to connect to the Internet using e.g. a DSL modem, select this setting. However you also need to enter your Internet access data in the settings under **Network – WAN**. Then restart the mbNET for the changes to take effect.
Connection monitoring	In addition, you can PING an IP address to verify an Internet connection's availability. You can set this up at different intervals for up to three different IP addresses.

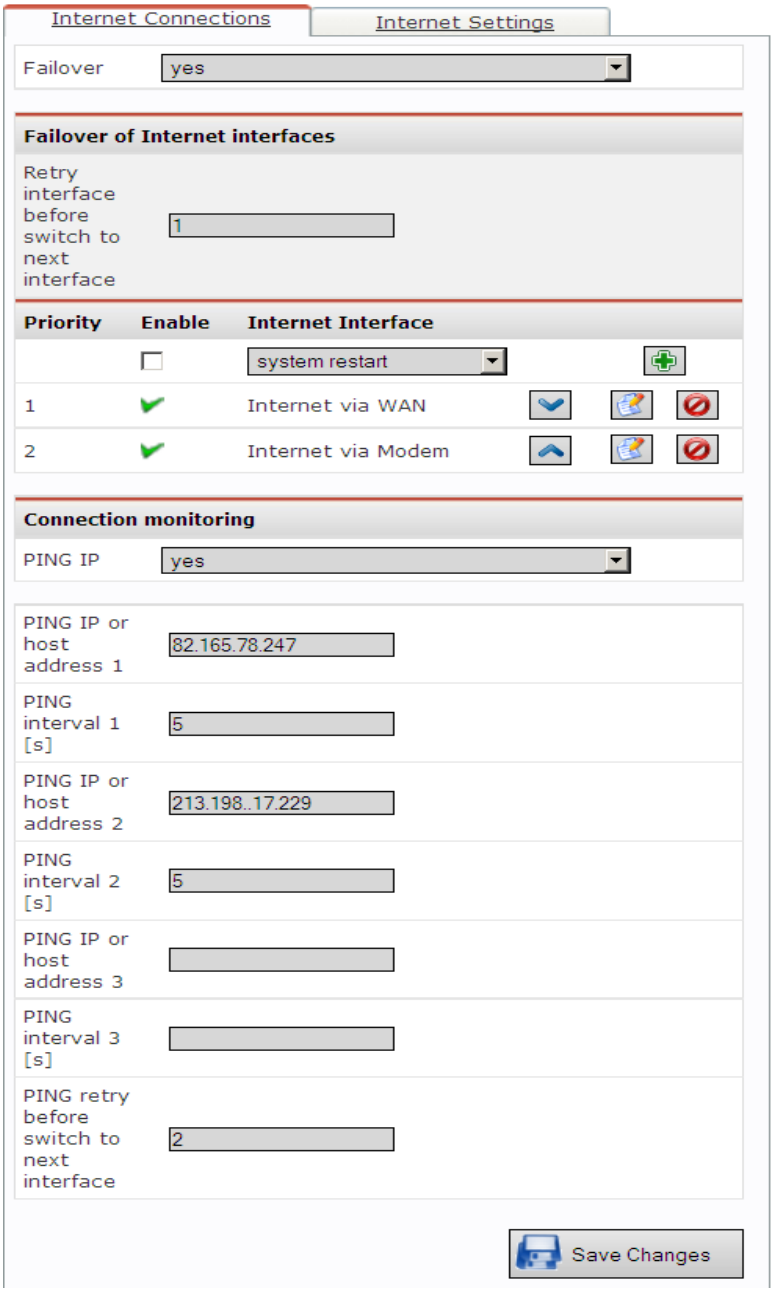
13.4.2 Network – Internet – Internet Settings

Label	Description
Connection Mode	❑ **Keep connection** Select this setting if the router should try to connect to the Internet immediately after restarting or after pressing the **RESET** button on the front of the router. **Important: with this setting, the connection will stay on** ❑ **On demand** Select this setting if you want the router to connect to the Internet when one or more of the options listed below are selected: ○ Connect while pushing **dialout button** ○ Connect when a signal is received at inputs **I1,I2,I3** or **I4** ○ Connect on traffic
Close connection if	❑ **Don't lock:** select this option if you want to prevent the Internet connection from being closed by a signal to a digital input. ❑ **Input1, Input2, Input3, Input4:** select this option if you want to be able to interrupt the Internet connection using a signal to one of the selected digital inputs.
Send IP address via email	Here, you can set whether to have an email containing the current public IP address sent to a pre-specified email address.
Email	If you select "send IP address via email", your need to enter your email address here. However you can also enter it manually in this field.
Settings	The **Settings** tab is only displayed if Internet connection via WAN or modem has been selected along with **On demand** for the connection mode. The following settings options will be displayed:
Connect on traffic	To connect to the Internet when a data packet is sent, check this box. In other words, an Internet connection will be established if the LAN is trying to contact a subscriber outside of the LAN.
Connect when pushing Dialout button	If you wish an Internet connection to be triggered by pressing the **Dial out** button on the front of the router, check this box.
Connect on Sign 1 at Input	❑ **Don't connect:** Select this option if you want to prevent the Internet connection from being triggered by a signal to one of the digital inputs.

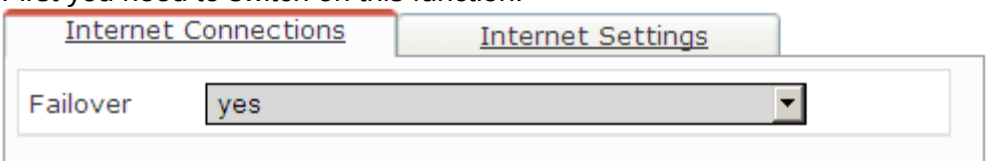
	❑ **Input1, Input2, Input3, Input4:** Select this option if you want to establish a connection using a signal to the selected digital input.
Close connection after ... [s] inactivity	Here, enter the length of time before the connection should be closed if the router has sent no further data packets in the interim. Leaving this blank switches off the function.

13.4.3 Internet failover connection

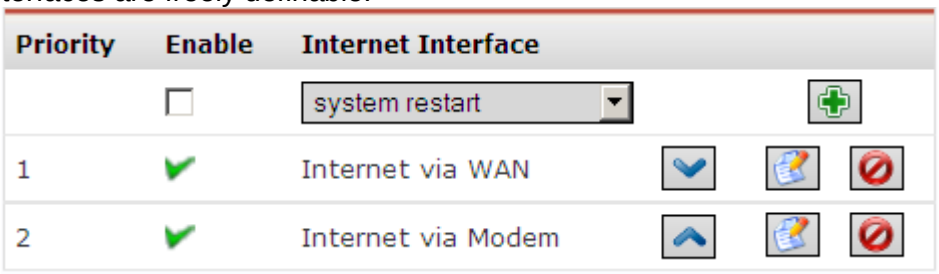
Firmware versions 3.x.x. and higher have an optional failover function for the Internet connection.



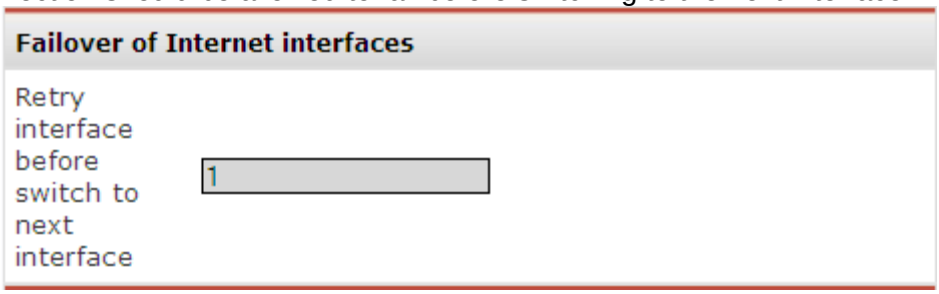
First you need to switch on this function.



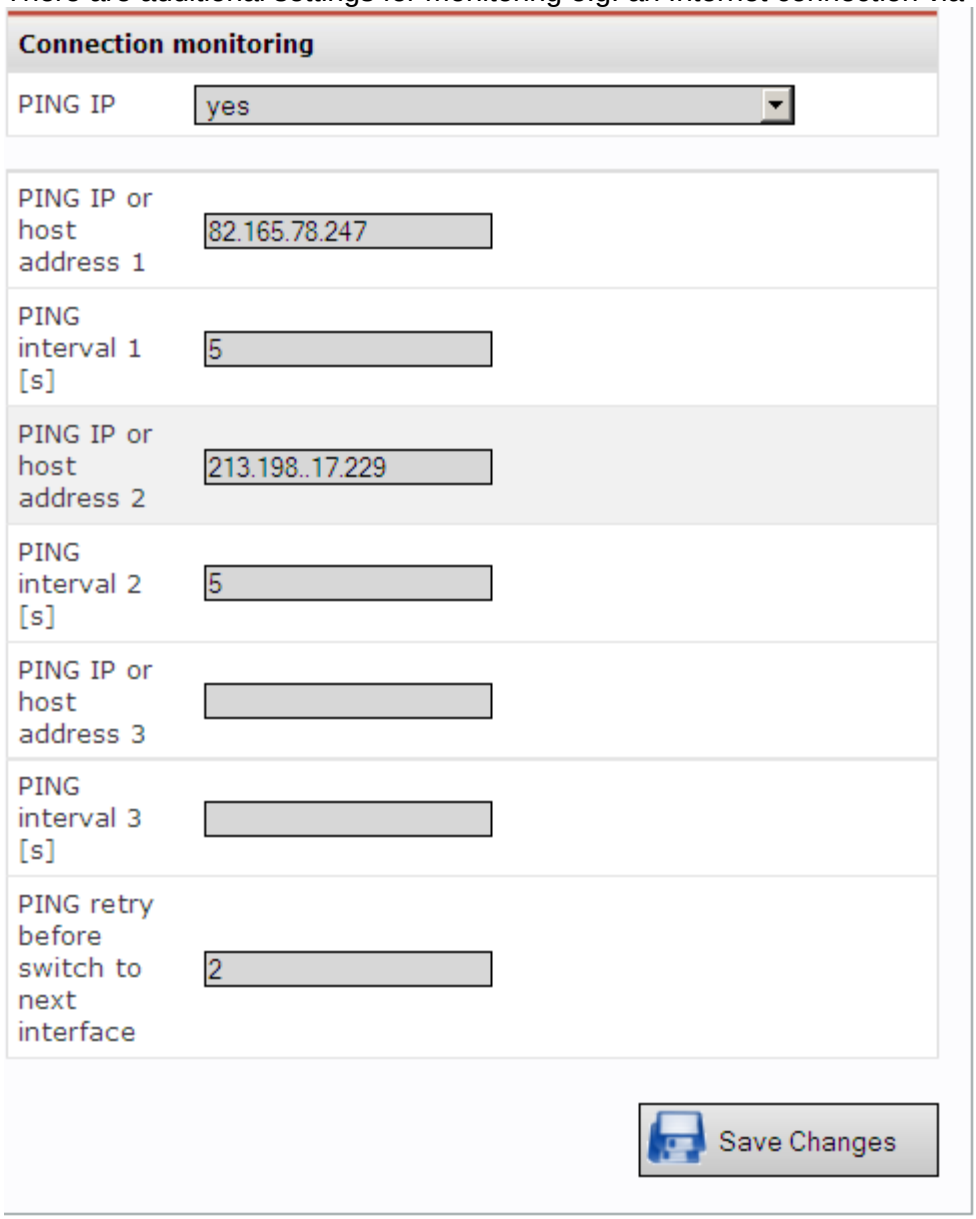
In the table below, you can select a priority order for the Internet interfaces. The order and number or interfaces are freely definable.



The "Retry interface before switch to next interface" parameter specifies how many times an Internet connection should be allowed to fail before switching to the next interface.

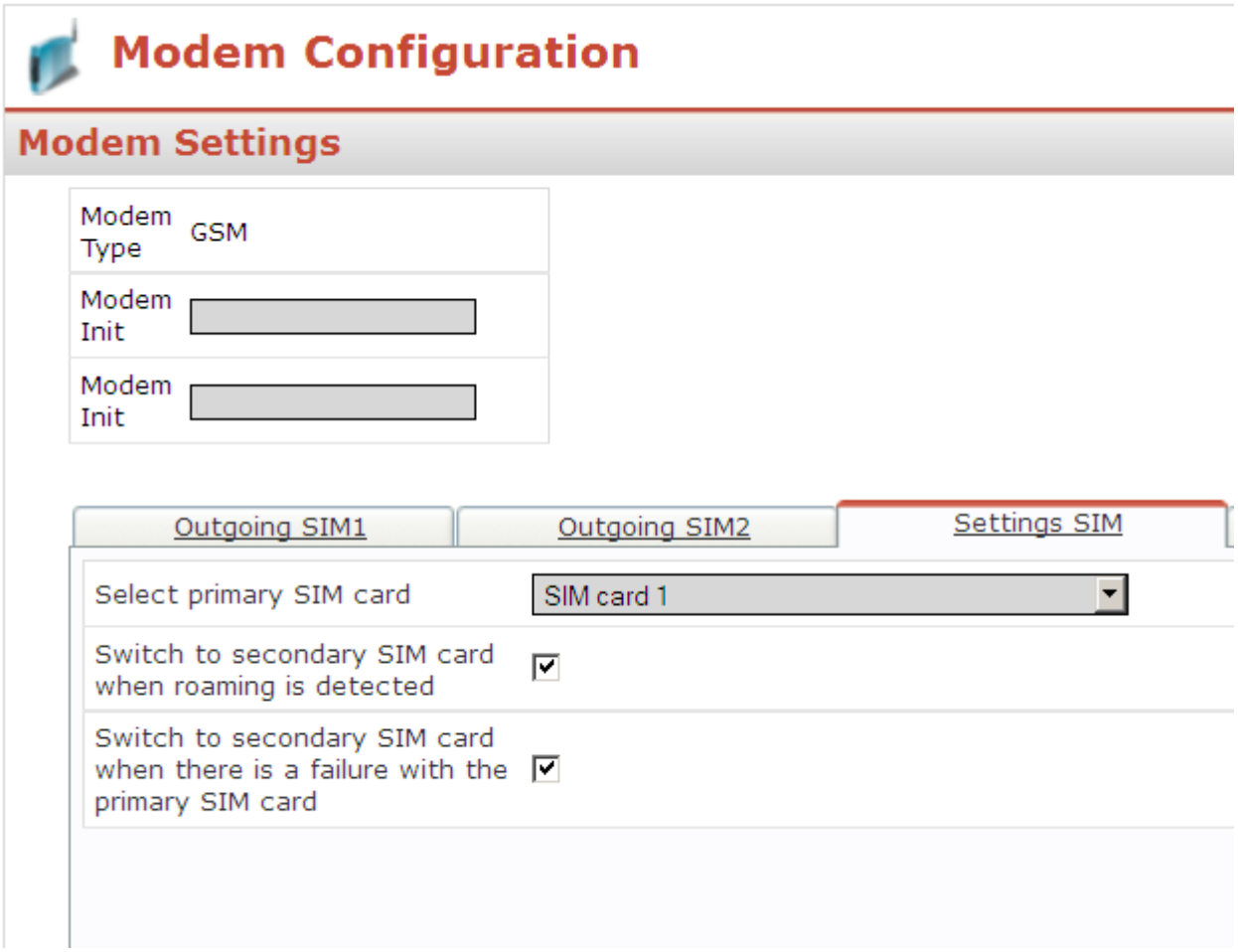


There are additional settings for monitoring e.g. an Internet connection via WAN



You can enter up to three different IP addresses which will then be run through in the following order. If the first IP fails, the second will be used. If this one also fails, the third will be used and once all three have been run through, a test will be carried out. If the set test retry limit is reached, the interface will switch. If the system gets to the last interface, it will start again with the first.

In addition, routers with a GSM/UMTS module and double SIM slot can switch between SIM1 and SIM2.



First, we need to specify a primary SIM card, which will always be verified or used by default. The secondary SIM card is always the non-primary one.
Switching is based on two (selectable) criteria:

- The SIM card fails to initialize, or to register on the mobile broadband network
- Roaming is detected on the SIM

13.5 Network – DHCP

You can configure the industrial router as a LAN or WAN DHCP server. DHCP enables you to integrate a new computer into an existing network without the need for any additional configuration. The only requirement is for the computer to be set up to acquire the IP address automatically.

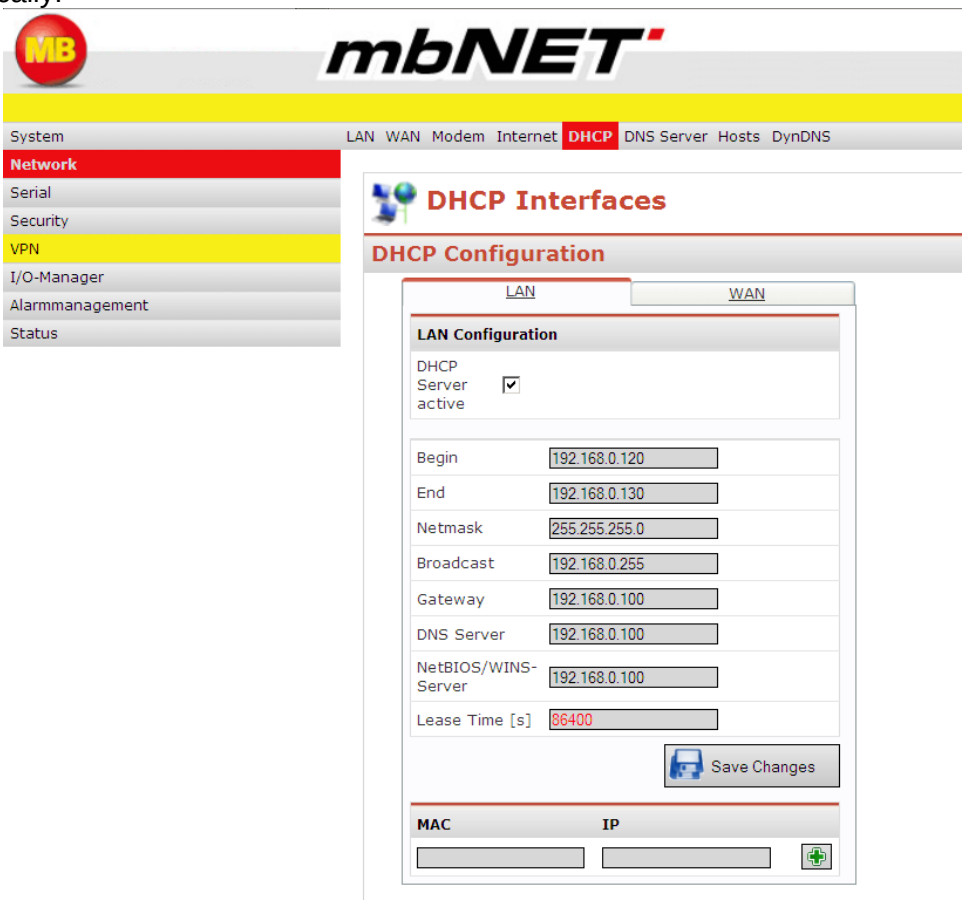


Figure 149

Label	Function
LAN – WAN	Selects to configure LAN or WAN interface.
DHCP Server active	Checking the box for this function allows the router to be enabled as a DHCP server for the relevant interface.
Begin	Enter the start address for the address range managed by the DHCP server here.
End	End address of the range managed by the DHCP server.
Netmask	Subnet mask of the range managed by the DHCP server.
Broadcast	Broadcast address of the range managed by the DHCP server.
Gateway	Optional entry. Here, you can enter the address of a router that connects network clients to the Internet or to another network. Here, enter the router's LAN IP address.
DNS Server	Optional entry of an existing network DNS server. Enter the router's LAN IP address here.
NetBIOS/WINS-Server	Optional entry of an existing network NetBIOS/WINS server.
Lease Time [s]	Length of time for which a client is allocated a specific IP address by a DHCP server.
MAC/IP table	Here, enter the fixed assignment between IP address and MAC address. In other words, you can specify that a device with a certain MAC address always receives the same IP.

13.6 Network – DNS server

DNS is used to resolve IP addresses to names.
The factory settings on the industrial router are configured so that the DNS server is assigned by the ISP. If you have a permanent industrial router connection, you can add a private DNS server here. This, rather than the ISP-assigned server, will then be the preferred server.

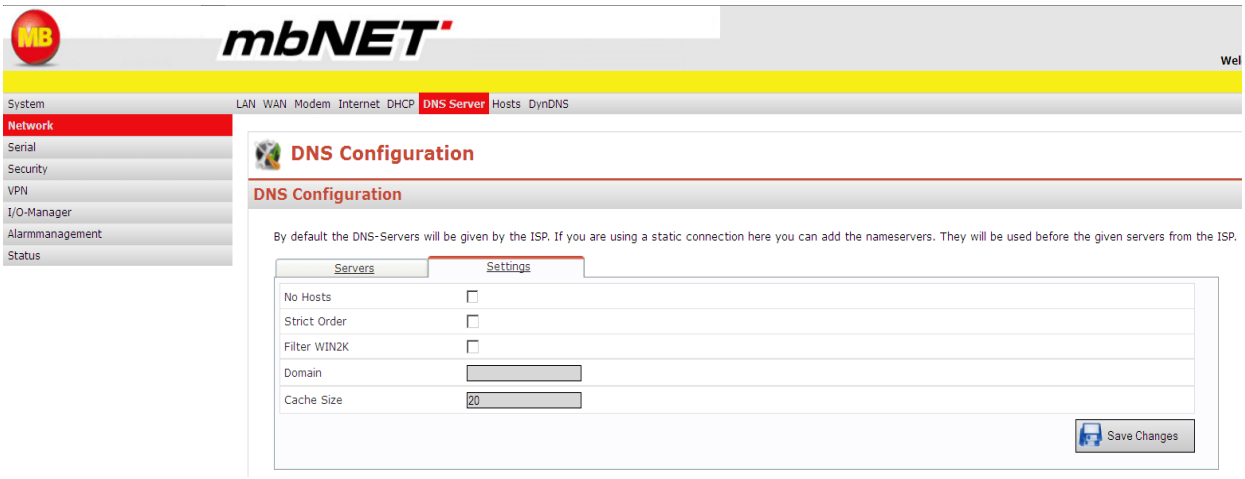


Figure 150

Label	Function
Servers	After clicking on this tab, you can enter an appropriate DNS server.
Settings	This tab allows you to activate or enter the DNS server settings listed below.
No Hosts	Computer names entered under the Network – Host menu are ignored.
Strict Order	The exact order set under "Servers" will be adhered to.
Filter WIN2K	Filters continuous and unnecessary requests from older Windows clients. This setting is useful when using a "on demand" connection as it avoids every re-quest resulting in a connection to the Internet.
Domain	You can enter what is known as a domain suffix here.
Cache Size	Input the number of cached names here, in other words, the number of names that are stored with IP addresses.

13.7 Network – Hosts

This setting allows you to allocate one particular IP address to a specific name, enabling a direct response to DNS requests. You can input and store, or delete, IP addresses and their associated names in these fields. This means that the mbNET must answer the request directly rather than forwarding the request to another DNS server.

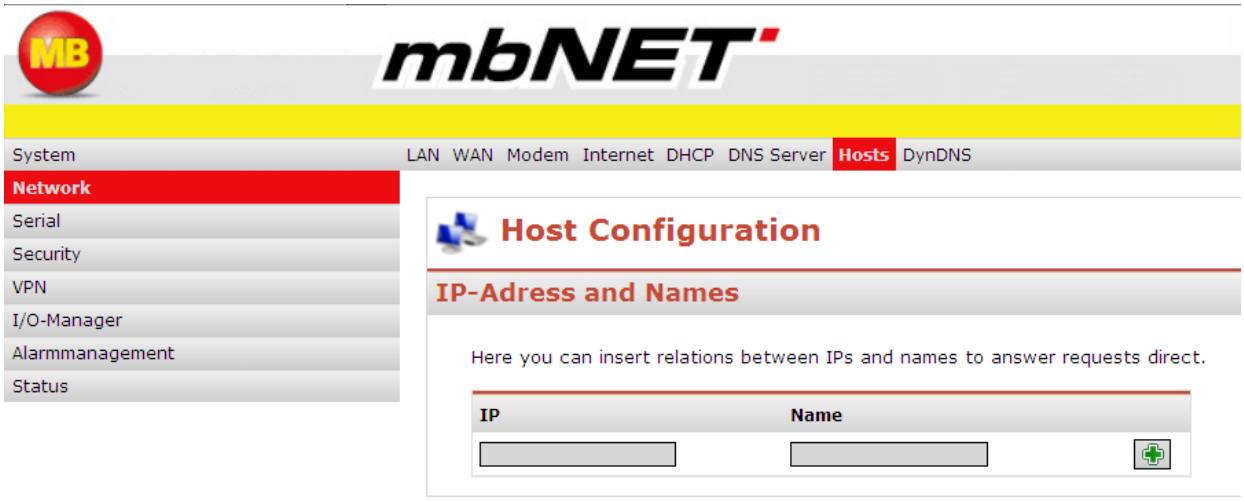


Figure 151

13.8 Network – DynDNS

13.8.1 General

As the industrial router is assigned a unique IP address whenever it dials in to the Internet, a client PC can locate it via this IP. However, as soon as it closes this connection and dials in again, it receives a new IP address. The DynDNS service makes the industrial router contactable using the same address every time. It resolves addresses to names and vice versa.

13.8.2 How to set up DynDNS configuration

A built in DynDNS service is included with firmware versions 1.4.0 and higher. This DynDNS service is operated by MB Connect Line. *No log in or registration is required.*

To use a public version of the DynDNS service you first need to register. Registration is usually free, and should not be particularly complicated.

If you are registered for a DynDNS service that is supported by the industrial router, you can input or select the options in the screenshot below.

Select **Network** – **DynDNS**
This will display the screen below:

Other services:
ez-ip: www.EZ-IP.Net
dyndns: www.dyndns.org
ods: www.ods.org
tzo: www.tzo.com
easydns: www.easydns.com
www.justlinux.com
dyns: www.dyns.cx
heipv6tb: www.he.net
dyndns-static: www.dyndns.org
dyndns-custom: www.dyndns.org
dhs: www.dhs.org

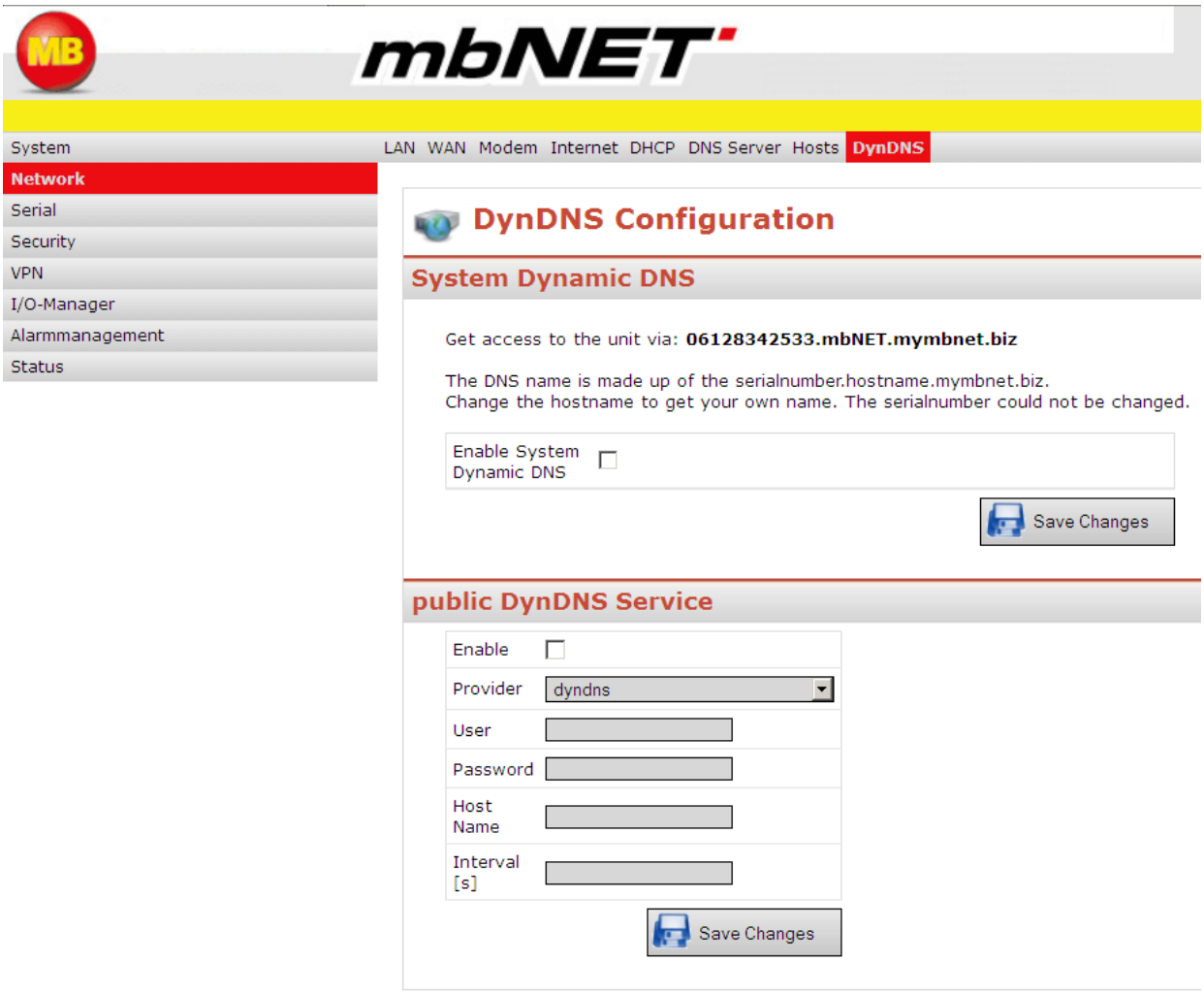


Figure 152

MB Connect Line DynDNS Service	
Label	**Description**
Enable system dynamic DNS	This option enables MB Connect Line's automatic DynDNS service. The name structure is fixed in this case, and can only be freely defined on one host: Name: Serialnumber.Hostname.mymbnet.biz The serial number is fixed and the host name can be anything you choose. Example: Device name: mbNET600 Serial number: 123456789 = Name on Internet: "123456789@mbNET.mymbnet.biz" The name will be globally available approx. 1-2 minutes after Internet dial-in.

Public DynDNS service	
Label	**Description**
Enable	If you are registered with a DynDNS provider that you wish the industrial router to use, check this box by clicking on it. The next time the industrial router dials into the Internet and receives a current IP address from the ISP, it will announce this address to the DynDNS service.
Provider	Using the drop-down field, select the name of the provider with whom you are registered, e.g. DynDNS.
User	Enter the user name that you used to register for the DynDNS service.
Password	Enter the password that you used to register for the DynDNS service.
Host Name	Enter the name that you assigned to the industrial router for the DynDNS service.
Interval[s]	This field is for whenever the industrial router name changes, e.g. after a new Internet dial-in. Enter the time interval after which the industrial router will inform the DynDNS provider of the new IP address.

14. Serial interfaces

14.1 General

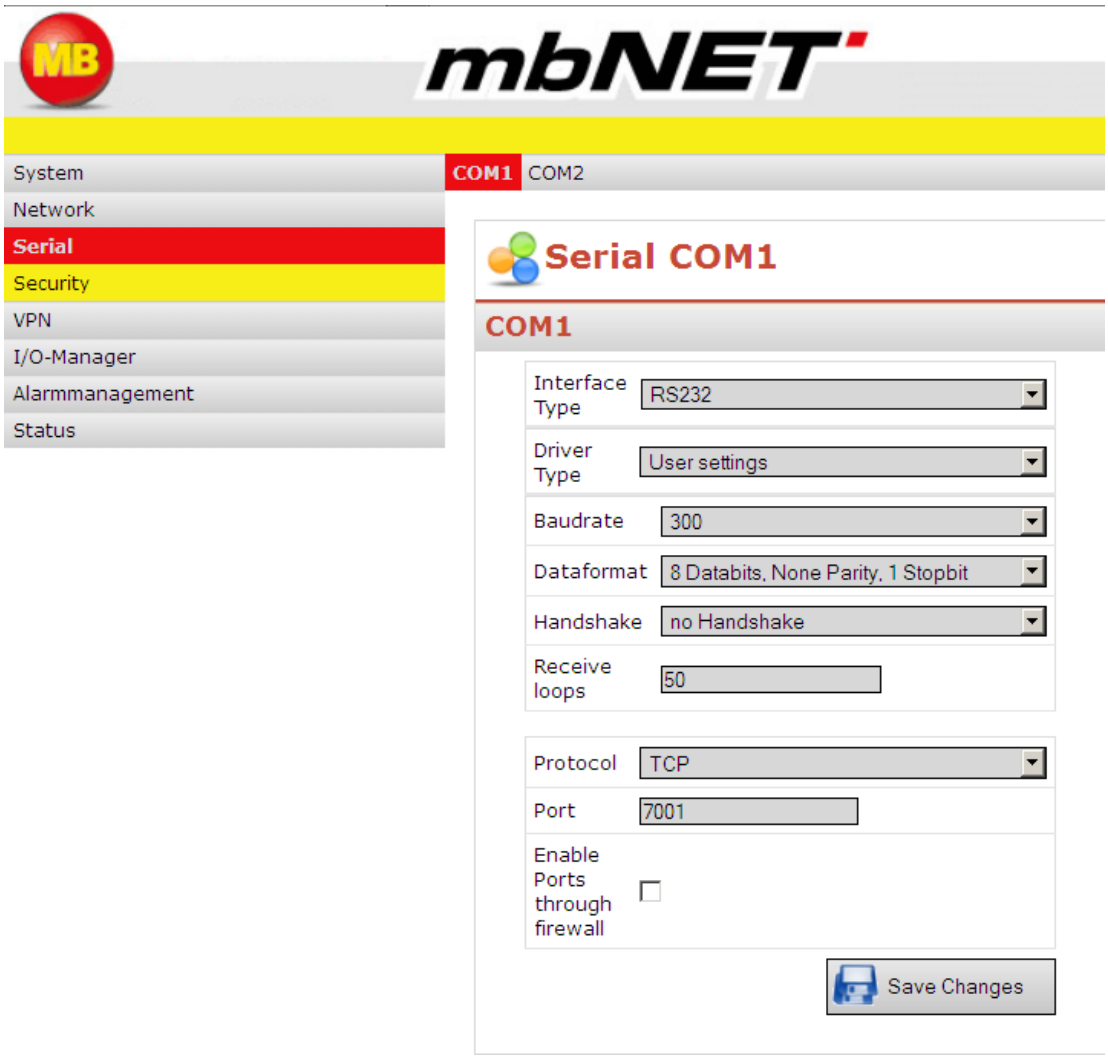
Both serial interfaces can be accessed via a dial-up or Internet connection using a known IP address.

Serial interface **COM1** can be directly configured to **RS232**, **RS485** and **RS422** using the web interface, and any associated control commands can be forwarded to the connected controller or device.

Depending on device model, **COM2** is an MPI/PROFIBUS interface on one model, and on other models it is the same as **COM1**. The MPI/PROFIBUS interface allows remote access to control systems e.g. S7-300/400, and supports baud rates of up to 12Mbit/s.

Clicking on the **Serial** button will display the following screen:

14.1.1 RS232/485 serial interfaces



Serial interfaces (continued)

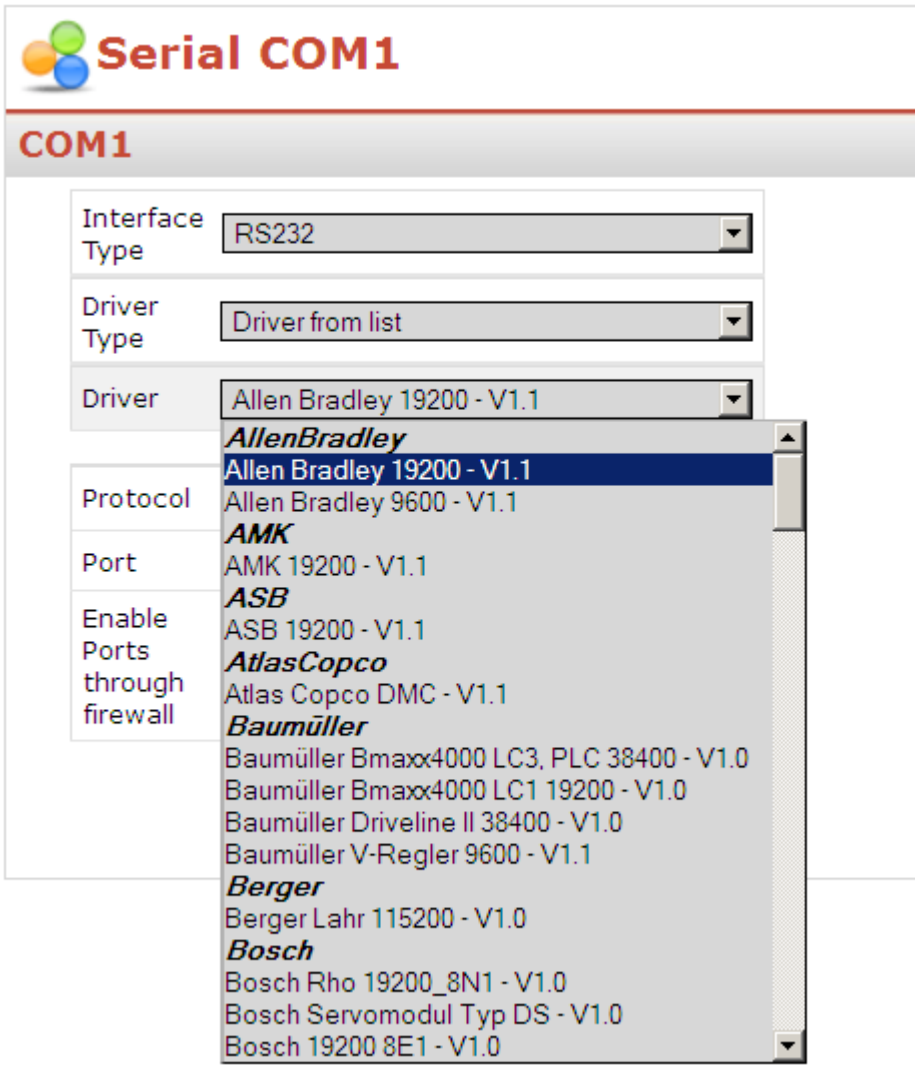


Figure 153

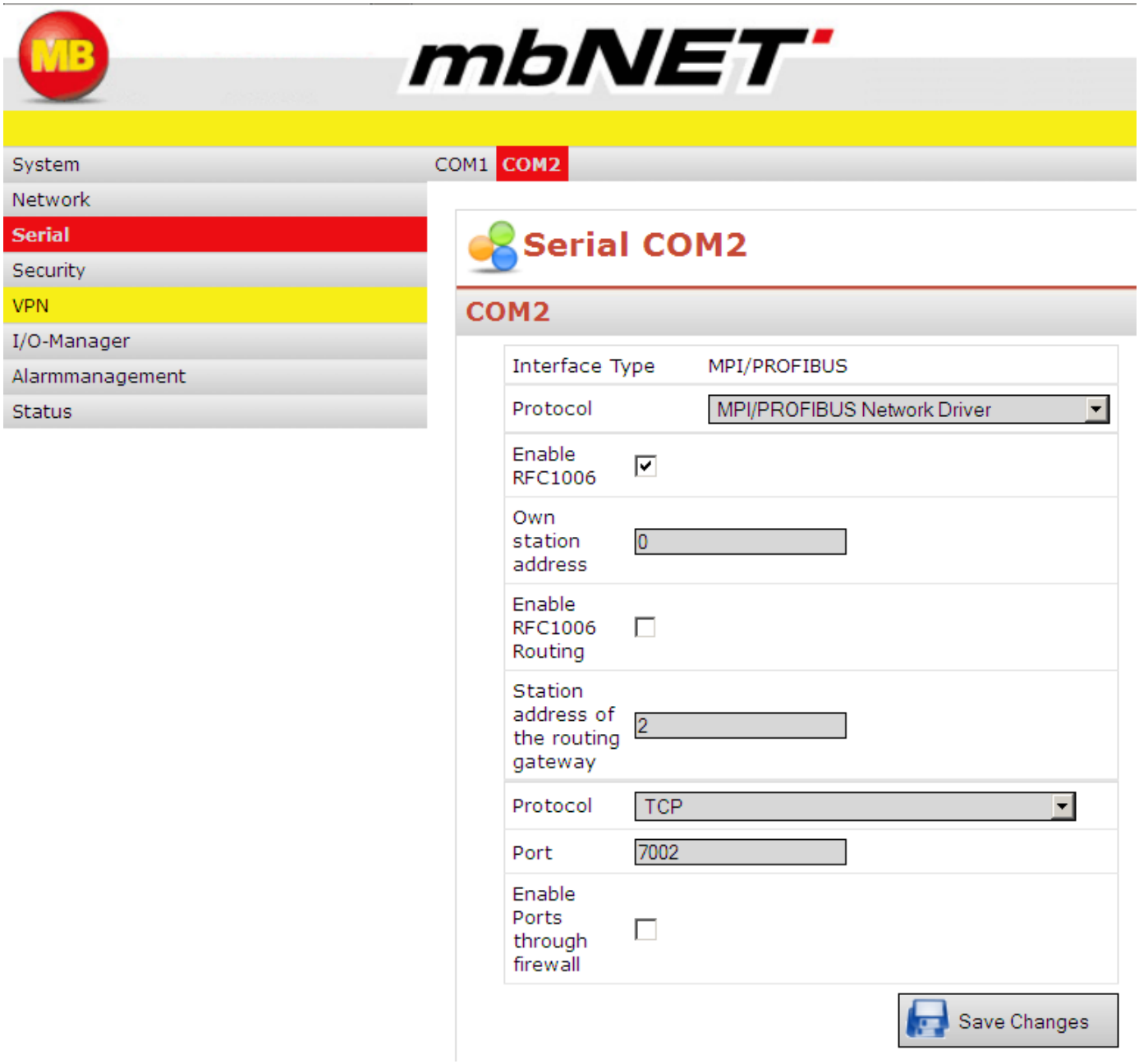
Label	Function
COM 1	Configuration options for COM1 interface The settings that follow it apply only to this interface.
Interface Type	Use this drop-down field to set the interface type for COM1. The options are as follows: RS232, RS485 2-wire, RS485 4-wire, RS422
Drivers	Driver from list: Select a product/brand-specific driver to control your serial device. User settings: If no suitable driver is available or you need to enter your own configuration parameters. These can be entered manually. Baud rate: Enter the baud rate for communication here. Data format: Select one of the settings for data bits, parity or stop

	bits Handshake: Select a handshake (flow control) option. Receive loops: This is a start counter for serial signals, i.e. how many cycles the system goes through until it sends the data packet.
Driver	Select the driver that you want to load. Device drivers can be selected for the following brands: AllanBradley, AMK, ASB, AtlasCopco, Baumüller, Berger, Bosch, B&R, DanfossVLT, Elau, F-Tron,GE_Fanuc, Hitachi, I-for-T, Indramal, IQ2000, KEB; Kuhnke, KEB, Lauer, Lenze, Locon, Micro_Innovation, Mitshubishi, Möller, Motoman, Npos, Omron, Parker Hauser CompaxC3, Phoenix, Pilz, PLC Direct, Primo, Proface, Promicon, Quin, SCS Automata, Seidel Kollmorgen, SEW, Siemens, Stoeber, Stromag, Sütron, Tsx37, Tsx47, Tsx57, Vectron, Vega Sensor, Voelkel Grenzlastregler, Winloc
Protocol	Select the protocol for communicating with the connected device. Options are: TCP and UDP
Port	Enter the port that will be used for communication.
Enable ports through firewall	Checking this box means that you can access the serial devices via the public address through the port assigned above, without being blocked by the firewall.

14.1.2 MPI/PROFIBUS interface

Communication with S7 via

- VCOMLAN2 (PC adapter in SIMATIC Manager)
- RFC1006
- mbNETS7 driver (direct installation in SIMATIC Manager)



Label	Function
Protocol	***VCOM-LAN2/PC adapter*** MPI/PROFIBUS Baud rate If you select "VCOM-LAN2/PC adapter", the PG/PC interfaces must be installed on a PC adapter (MPI/PROFIBUS). For bus speeds higher than 1.5 Mbit/s this must be manually assigned. ***MPI/PROFIBUS network driver***

	Note: enabling this option launches the installation of network drivers on the client PC. Dispensing with separate driver installation and using the "TCP/IP (Auto)" option with a PG/PC interface is only possible if the RFC1006 option is enabled. Instructions on this are available on our website support pages under the heading "RFC1006". RFC1006 uses TCP Port 102. Enable RFC1006 You can select to enable the RFC1006 protocol here. Own station address If RFC1006 is enabled, assign a unique MPI/DP station address for the router. *Note:* the connected router will use this station address to log into the MPI/DP network. This is necessary if you are using RFC1006 communication exclusively. In a mixed operation of connections using network drivers and RFC1006, the router always logs in using the address assigned to the first connection used. Enable RFC1006 routing This option enables routing via RFC1006. Station address of the routing gateway If RFC1006 routing is enabled, you must enter the address of the routing gateway (14 – see example below) *Note:* to access a slave subscriber station in a subnetwork that is not directly connected, the master gateway must be assigned as the PLC routing gateway station address on the router. *Example:* The PLC (master) is connected to the router (e.g. address 13) via MPI Bus (e.g. address 14) and a subscriber station (e.g. address 5) is connected to the master PROFIBUS (e.g. address 4). To now be able to access the subscriber with address 5 on the PROFIBUS via the router (13) using MPI, routing needs to be enabled. **More information on installation is available via our Support Portal at www.connectline.com**
MPI/PROFIBUS baud rate	Select from the following options: PG/PC Interface Settings, 3Mbit/s, 6Mbit/s and 12Mbit/s
Protocol	Select the protocol for communicating with the connected device. The following options are available: TCP and UDP
Port	Enter the port that will be used for communication.
Enable ports through firewall	Checking this box means that you can access the Internet through the port assigned above, without being blocked by the firewall.

With firmware version 2.0 or higher, the RxD2 LED lights up when a MPI or PROFIBUS connection is established, and the TxD2 LED flashes when data is being transferred over either of these connections.

Redirecting serial interfaces to your PC (VCOM LAN2)

To make serial interfaces (including MCI/PROFIBUS) available on your PC, you need the VCOM LAN2 software utility. VCOM LAN2 can be downloaded free of charge from www.mbconnectline.de. VCOM LAN2 installs two virtual COM interfaces on your client PC. Data is then exchanged over these virtual COMs

COM 7 <> COM 1
COM 8 <> COM 2

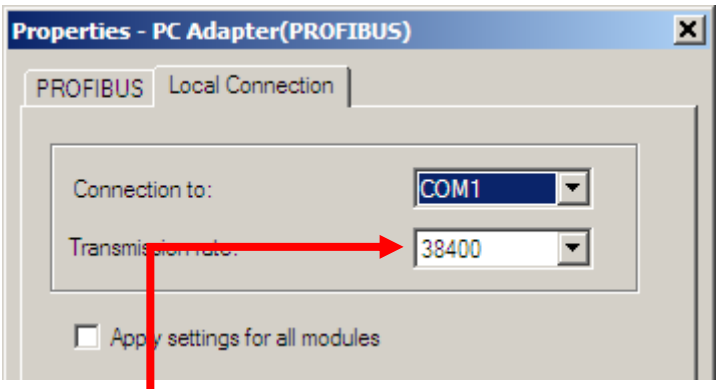
Run the VCOM LAN2 set up file and follow the installation instructions.
When installing a system you should be aware that the ports (**TCP/UDP 254000 and 25401, depending on settings**) are enabled on both client side and router side. Note also that if you select the connection setting "connect when the virtual COM-Port was opened from an application program", a small amount of data may be lost while the virtual COM port is being opened, as some programs send data to the port immediately, before the virtual COM port has established a connection.
More information is available under VCOM LAN2 program Help.

14.1.3 Settings for Simatic Manager

If you wish to set up a connection to a Siemens control system, you first need to verify the settings in Simatic Manager by selecting

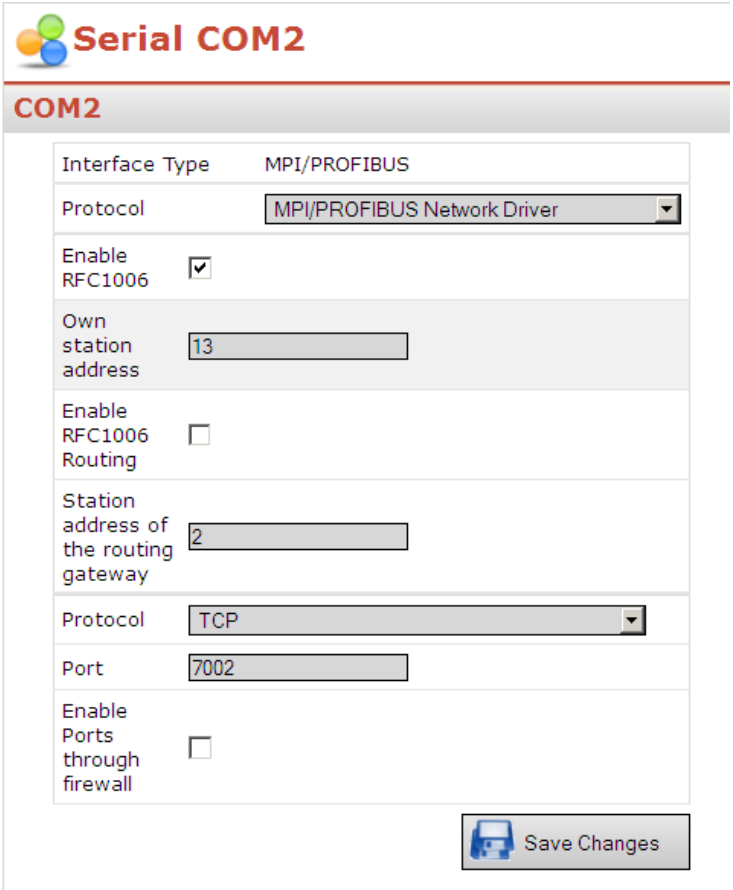
Extras → Set up PG/PC interface → PC adapter (PROFIBUS) or *PC adapter (MPI)*

and then clicking on Properties. This will open a menu screen with a "Local Connection" tab. The transmission rate here **MUST** be set to 38400.



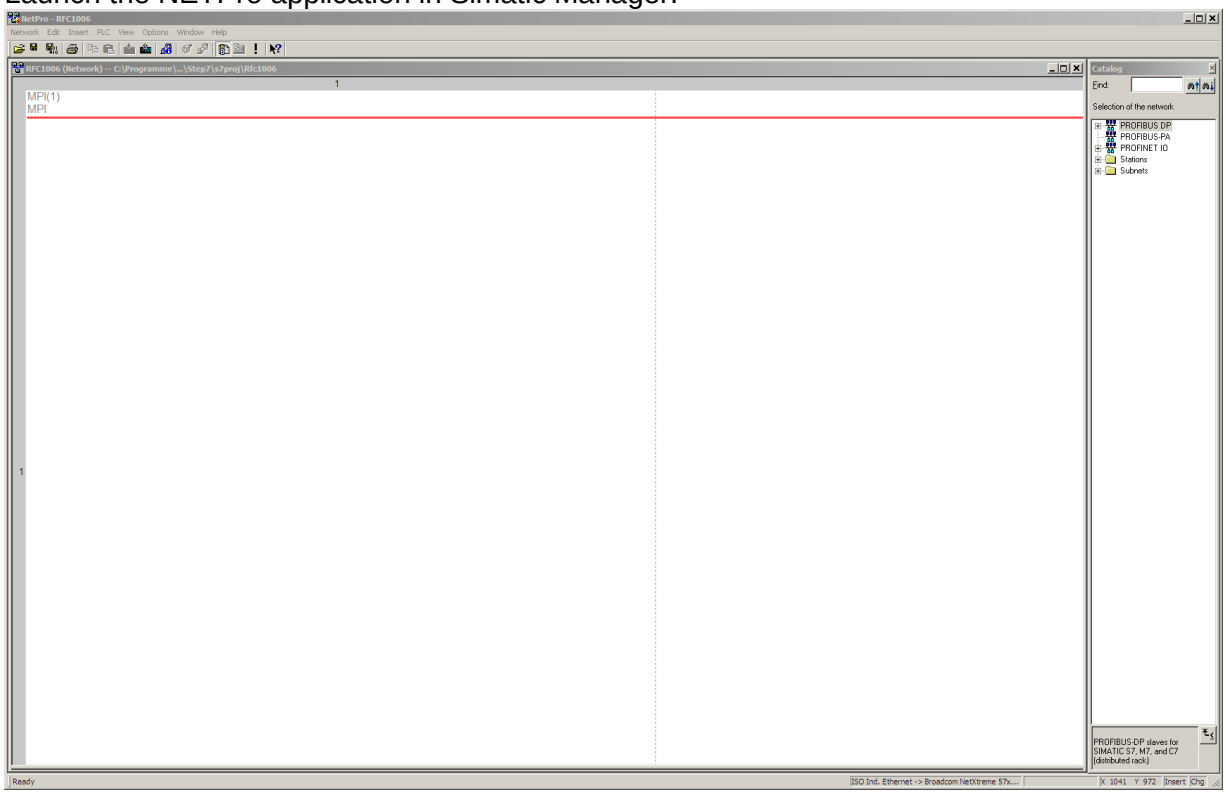
14.2 Enabling RFC1006 on the mbNET

Enable the RFC1006 option under the "Serial Interfaces", "COM2" menu. Specify the own station address for the mbNET.



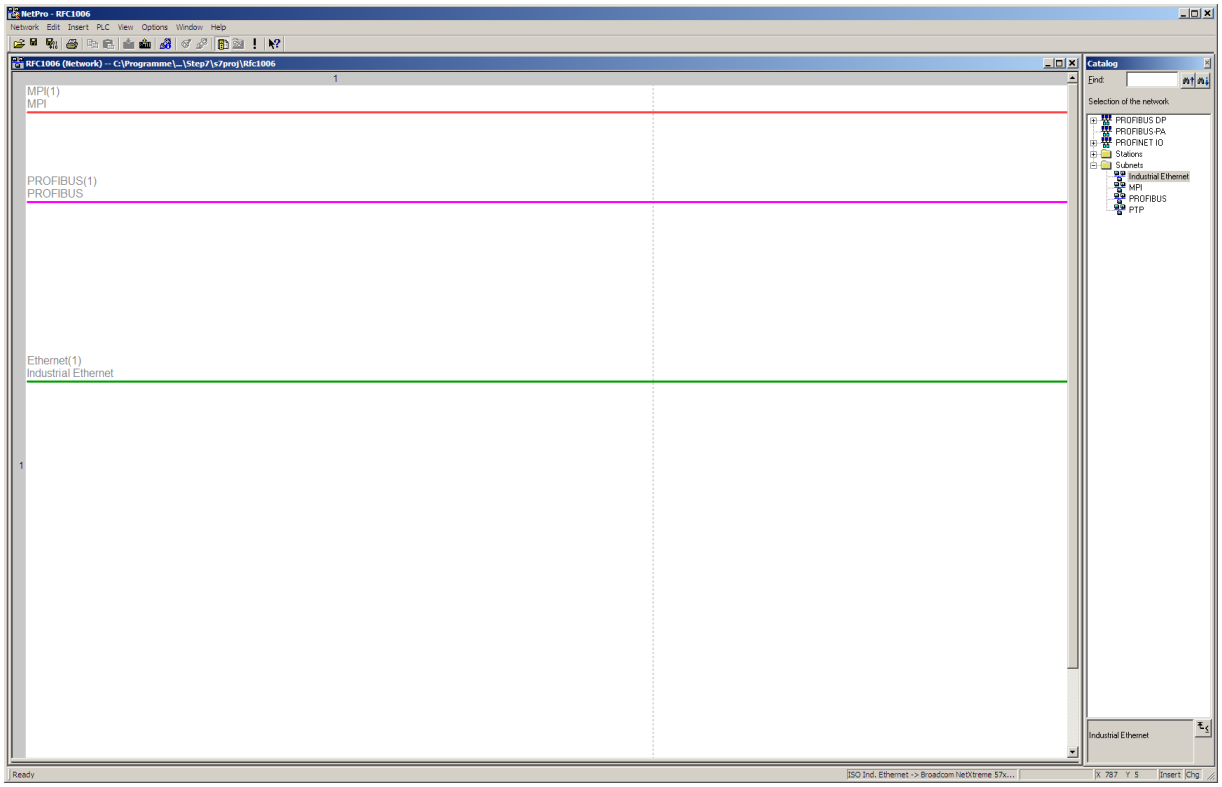
14.2.1 **Settings for NETPro Step 7**

Launch the NETPro application in Simatic Manager.



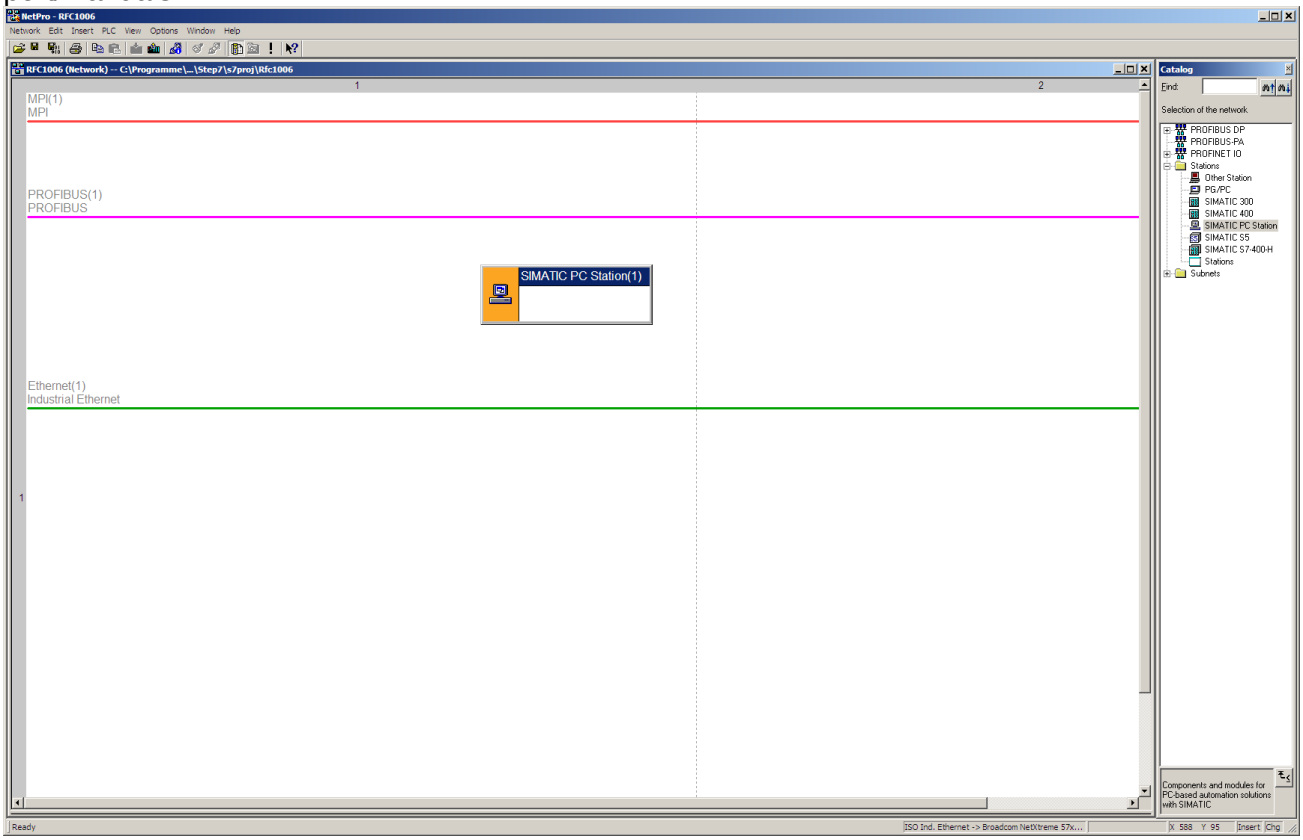
14.2.2 **Create subnets**

Create a "PROFIBUS" and an "Industrial Ethernet" subnet.



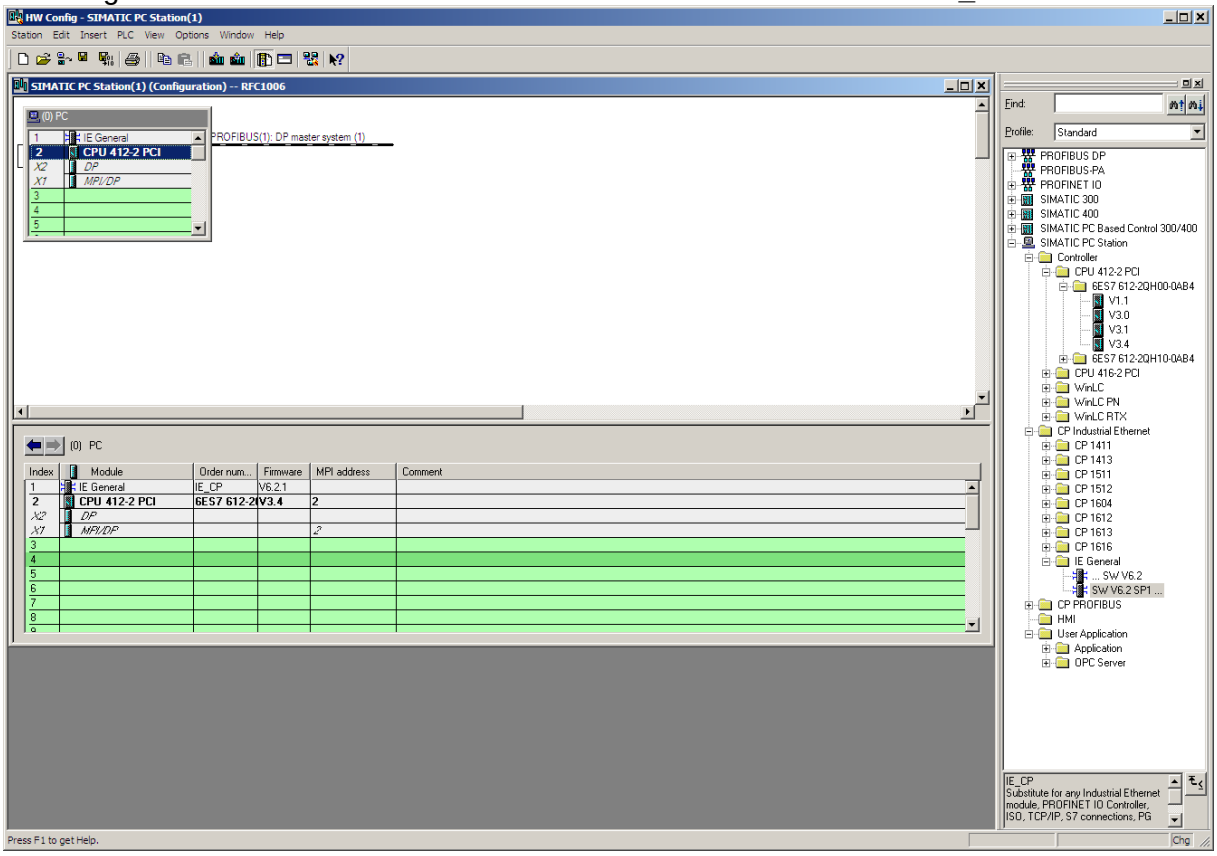
14.2.3 **Add PC station**

Following step 2.1 you need to add a PC station. You can skip steps 2.2 to 2.3 if you are using the "*NETPro*" Import function. A pre-configured mbNET station is available as an annex to these instructions. You can download this as a Zip file from our homepage http://www.mbconnectline.de under Support/Manuals.



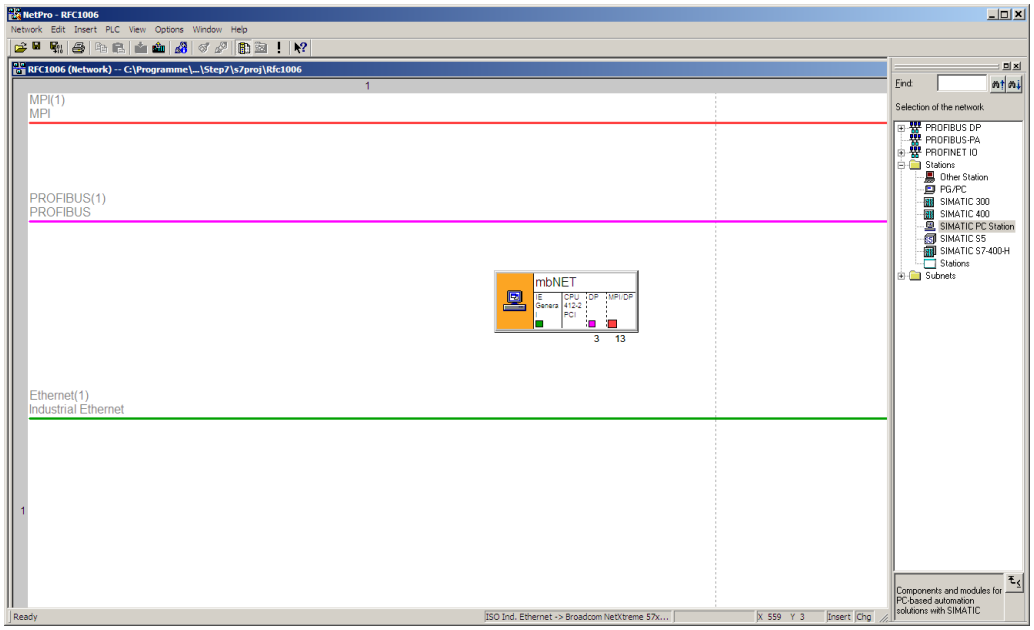
14.2.4 **Configure PC station**

This "*PC Station*" requires the integration of a "*CPU 412-2 PCI (6ES7 612-2QH00-0AB4 V3.4)*", found by selecting "*Simatic PC Station -> Controller -> CPU412-2 PCI"* and a "*IE_CP V6.2.1 (IE General)*" found by selecting "*Simatic PC Station -> CP-Industrial Ethernet -> IE General-> IE_CP SW V6.2 SP1*".

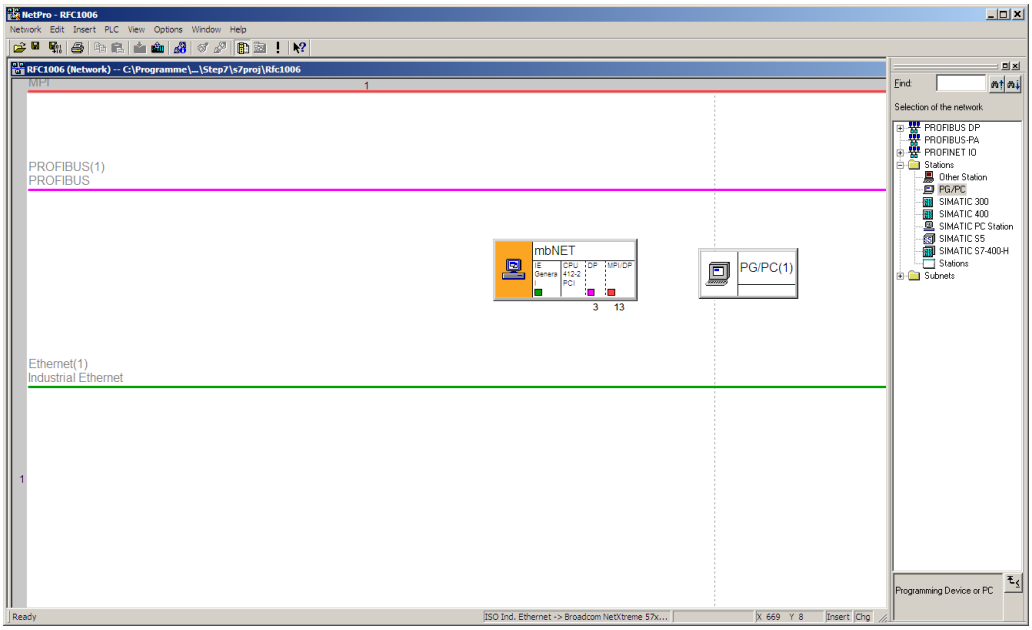


The finished station must now be saved, and appears in "NETPro".
The MPI/DP address must match the settings entered in "own station address" on the mbNET.

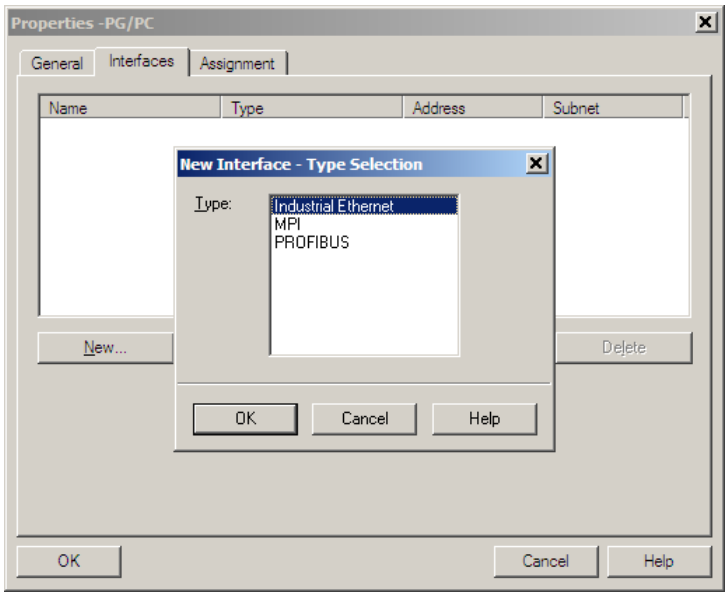
14.2.5 **Add PC/PG station**



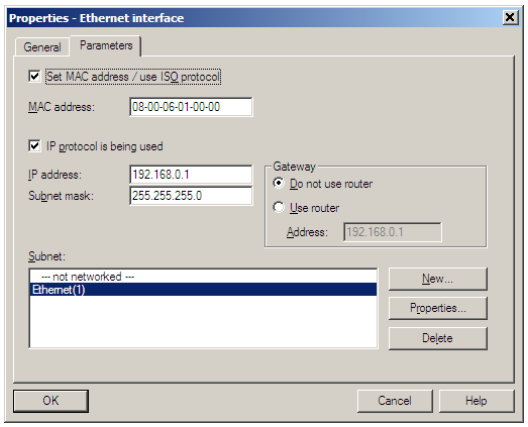
Now you need to add a PC/PG station.



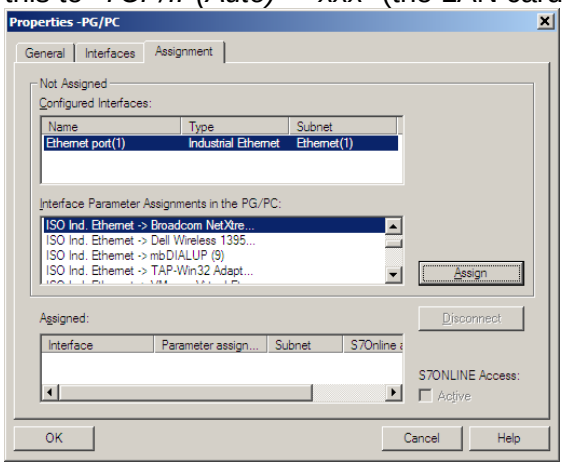
Double clicking on "*PG/PC Station*" opens the Properties window for this. Here, you need to add this interface by selecting "*Interfaces -> New …-> Industrial Ethernet*".



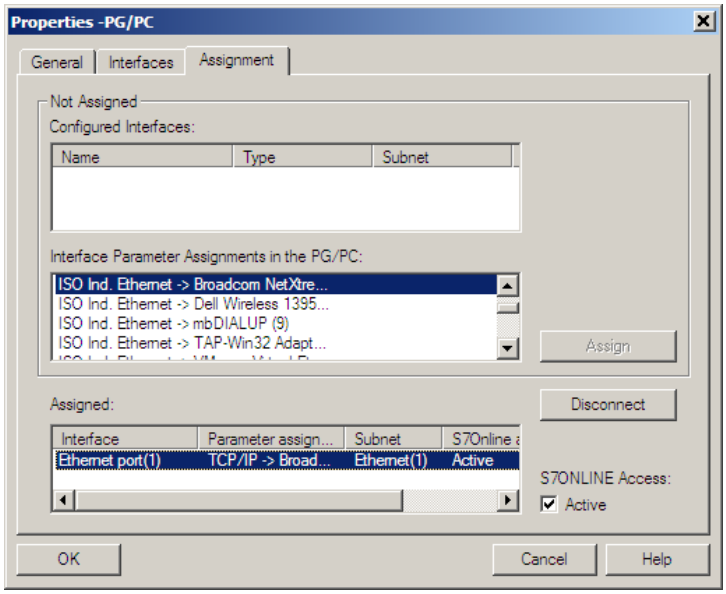
This opens a window where you need to make the "*Industrial Ethernet*" settings for the PC.
Specify the PG/PC subnet mask and IP address here. The PG/PC IP address can be from anywhere in the network range but may not overlap with other addresses on the network and must not be the real IP address of the PG/PC.



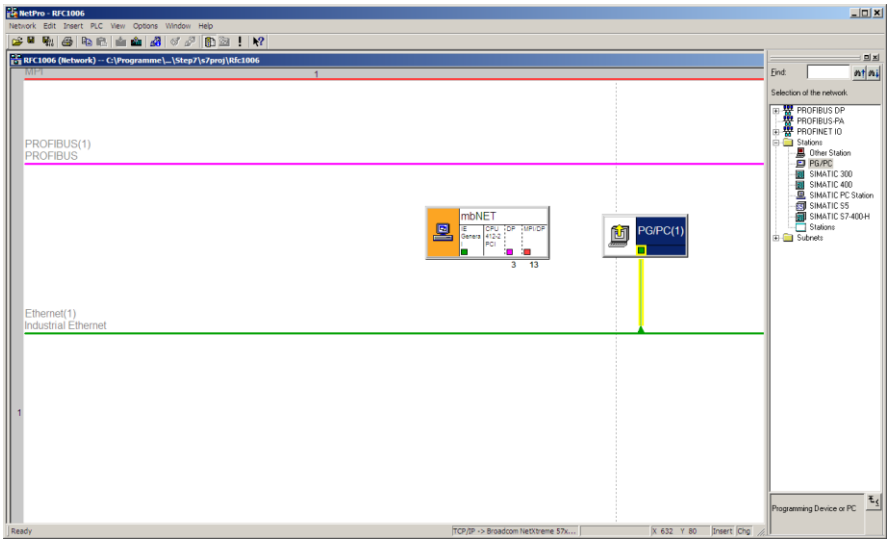
Next, in the "*Assignment*" tab, find the interface that you intend to use as the "Ethernet Interface" and link this to "*TCP/IP(Auto) -> xxx*" (the LAN card in use) by clicking on the "*Assign*" button.



After assigning your chosen interface, the window should look like this. S7ONLINE access must be set to "Active".

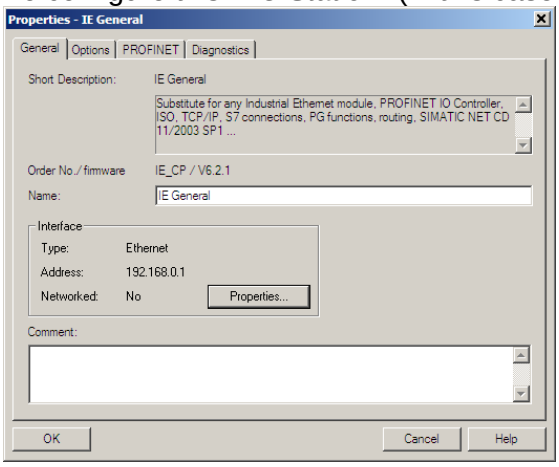


The subnet *"Industrial Ethernet" is now linked with the PG/PC*.



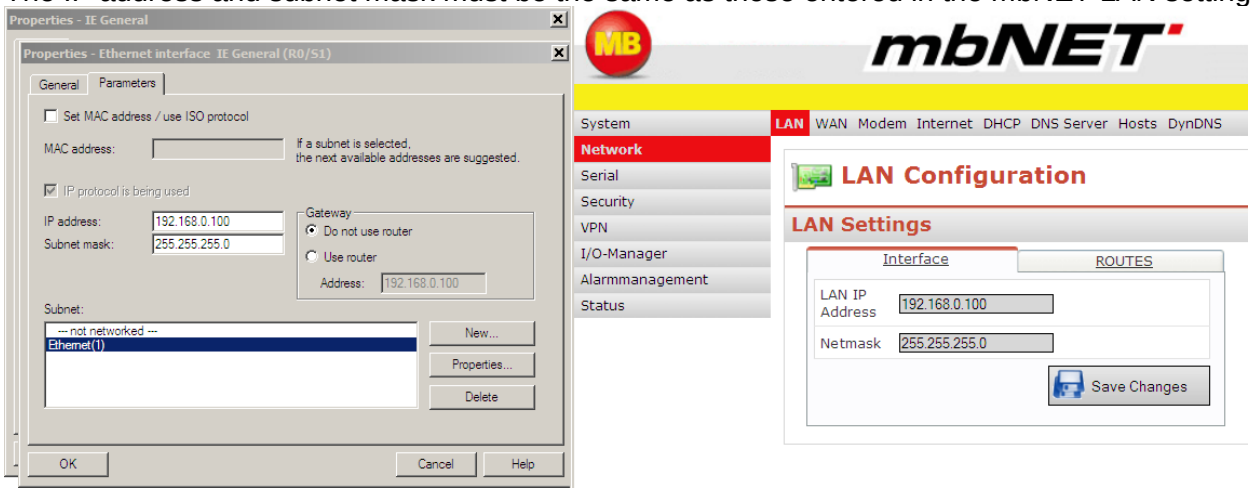
14.2.6 **Configure mbNET PC station**

To configure this "*PC Station*" (in this case: mbNET), double-click on "*IE General*".

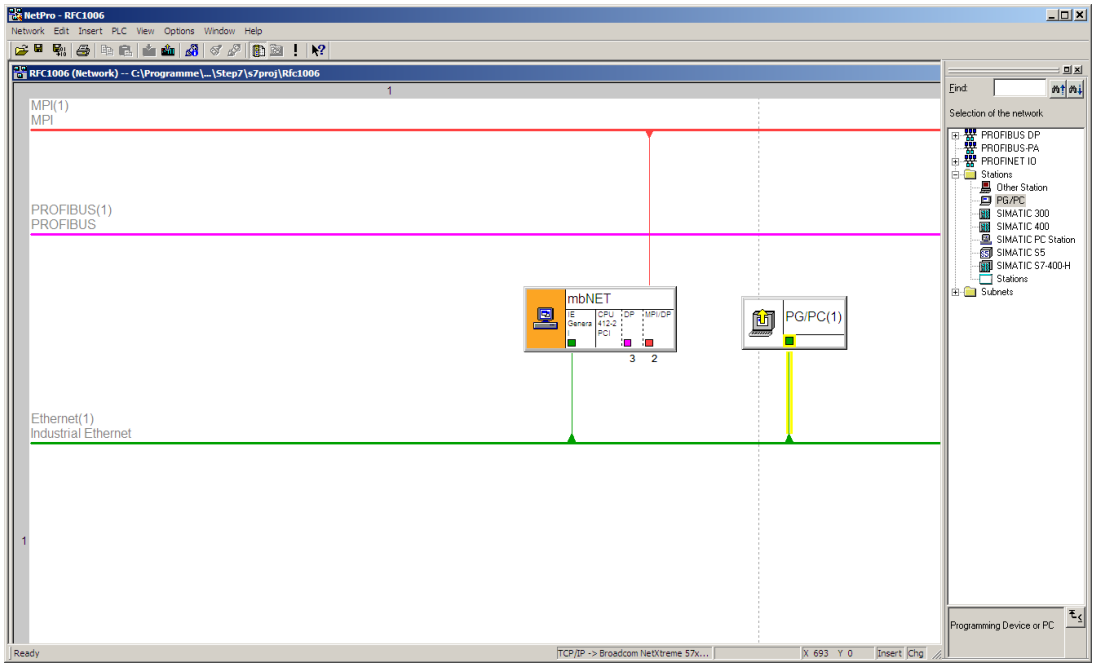


Click on "*Properties*" to set the interface parameters. Enter the IP address and subnet mask here.

The IP address and subnet mask must be the same as those entered in the mbNET LAN settings.

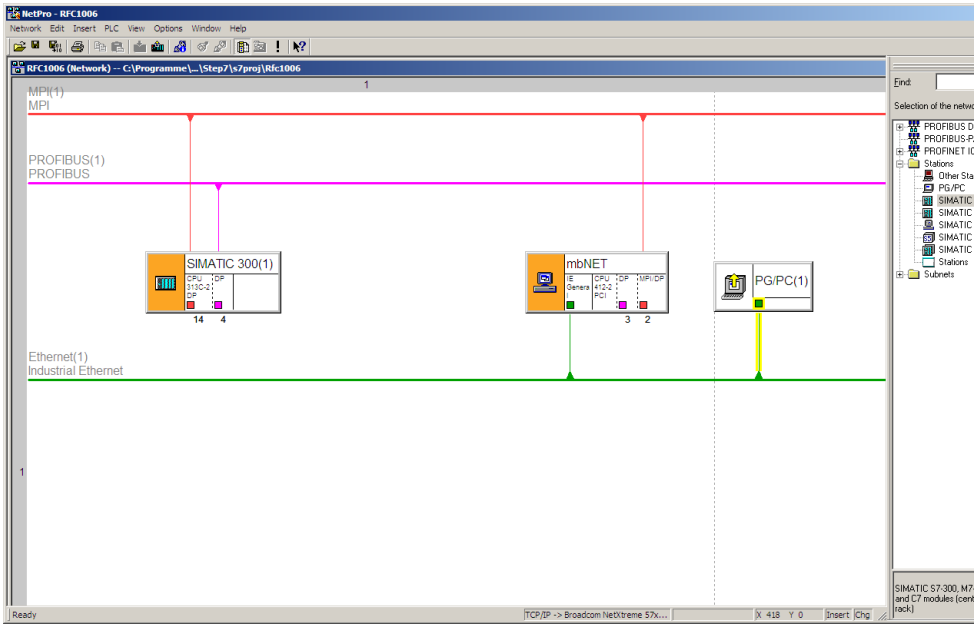


The main "*NETPro*" window should now look like this.

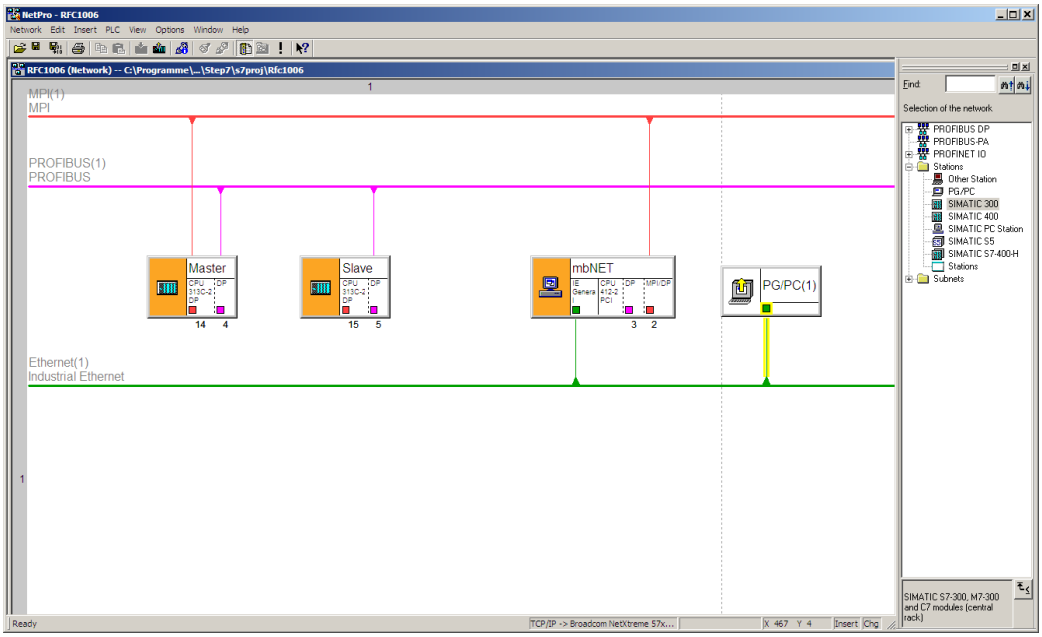


If everything has worked as it should, then "*TCP/IP(Auto) -> xxx*" (network card) will appear in the bottom border of the screen as "*PG/PC interface*". It is recommended at this stage to assign a bus address (in this case, MPI) to the PC station and link this with the subnet.

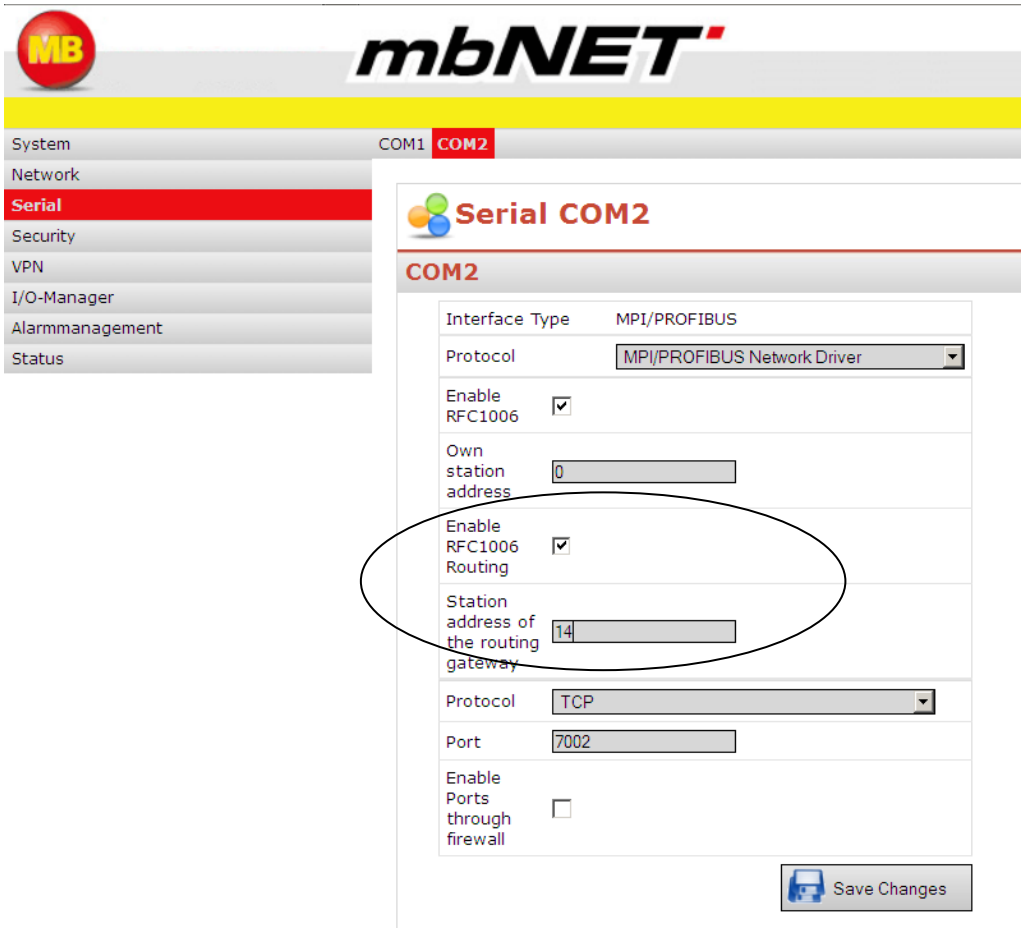
Finally, a CPU of your choice can be added to the relevant subnet.
The example here uses a *"CPU 313-C2DP"*



Routing
For the station to be able to contact a subscriber from another (slave) network (see picture), you need to make the following settings.

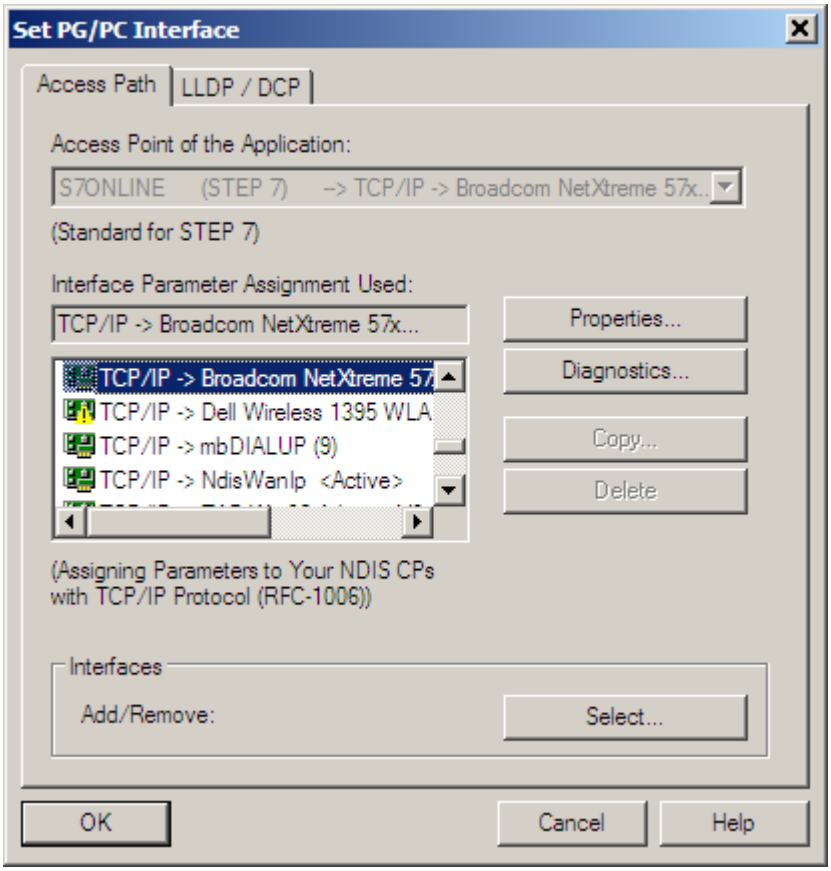


In the mbNET settings, enable RFC1006 routing and enter the station address of the (master) routing gateway.

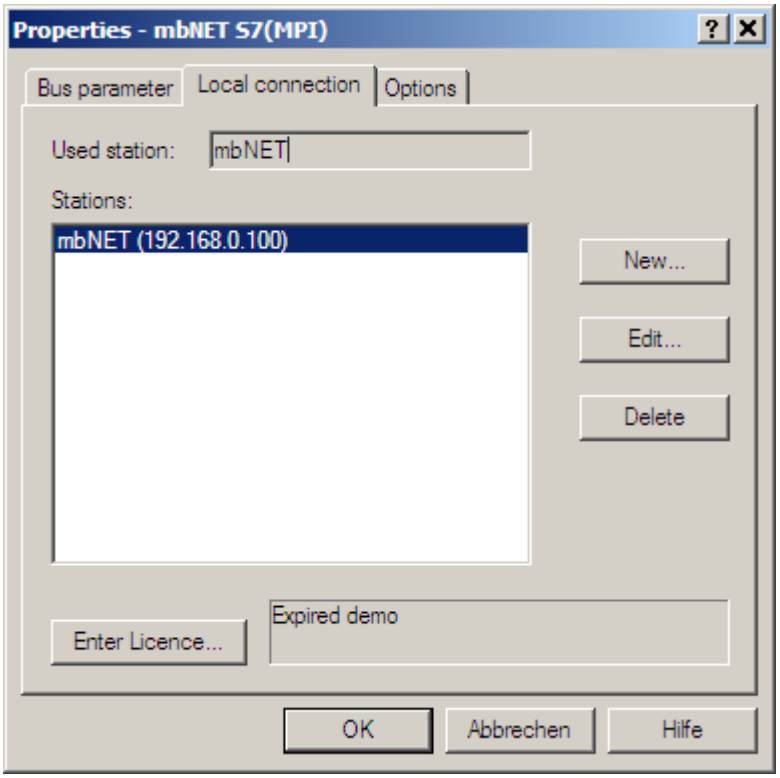


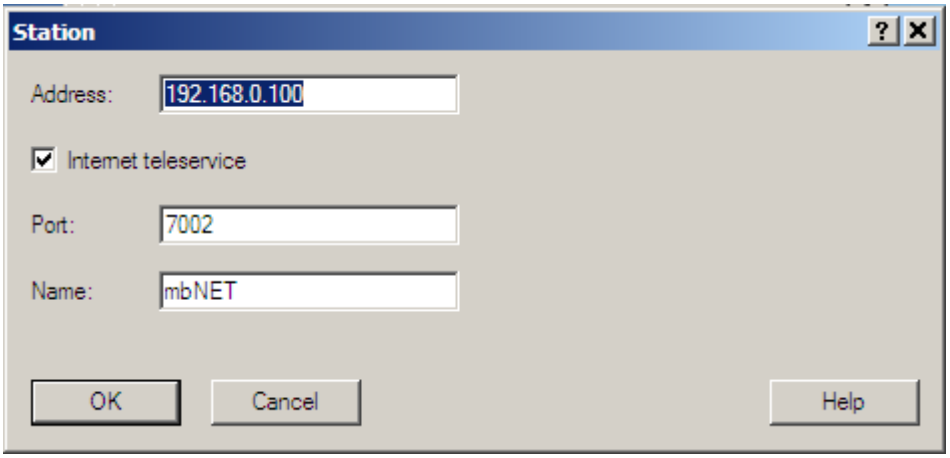
14.3 Connecting to S7 using the mbNET S7 driver

Alternatively, the licensed mbNET S7 driver can be used. Once installed, this is directly available as an adapter in Simatic Manager.

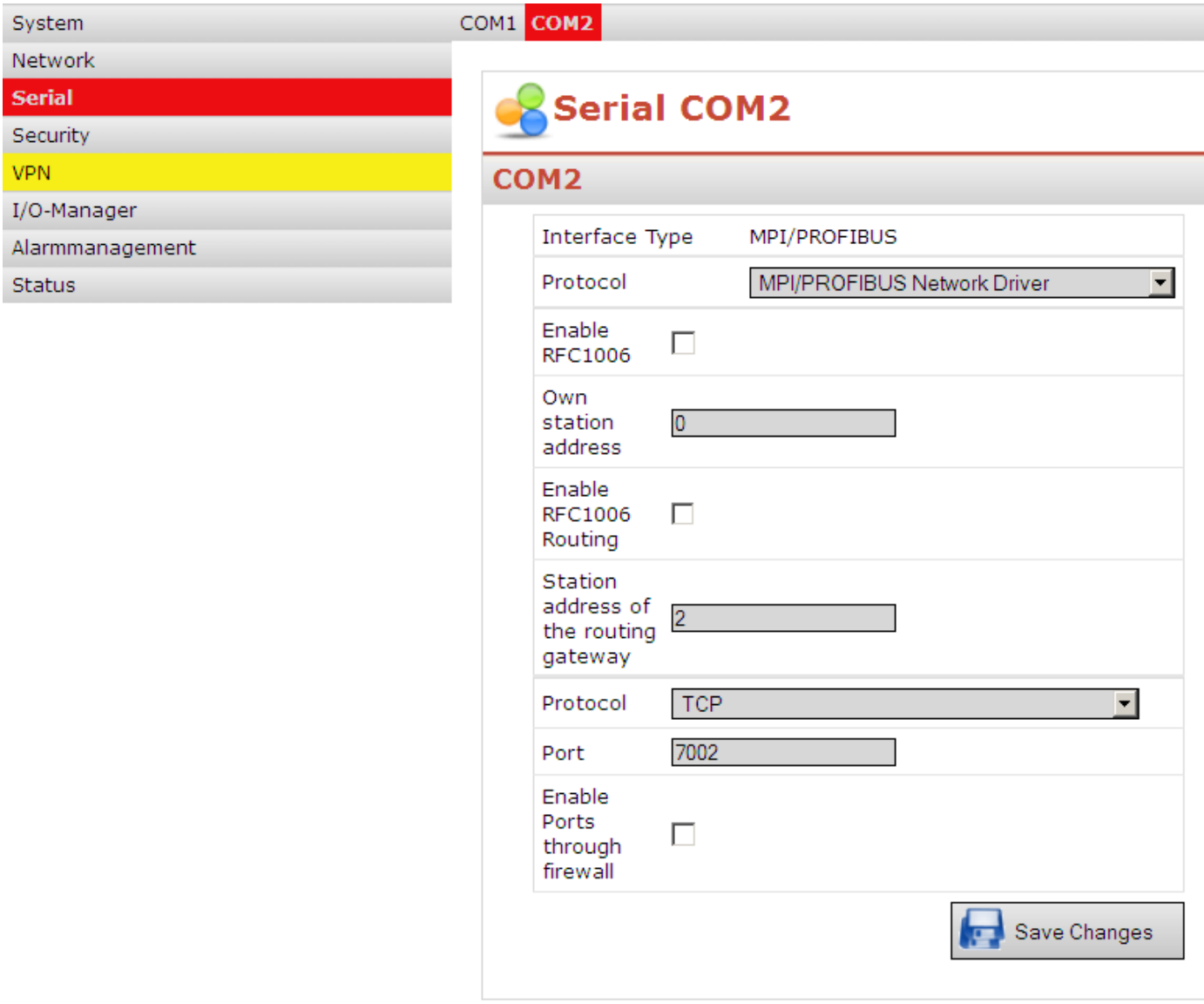


Setting the router IP address then becomes an overall project setting in the driver properties, rather than setting it project by project.





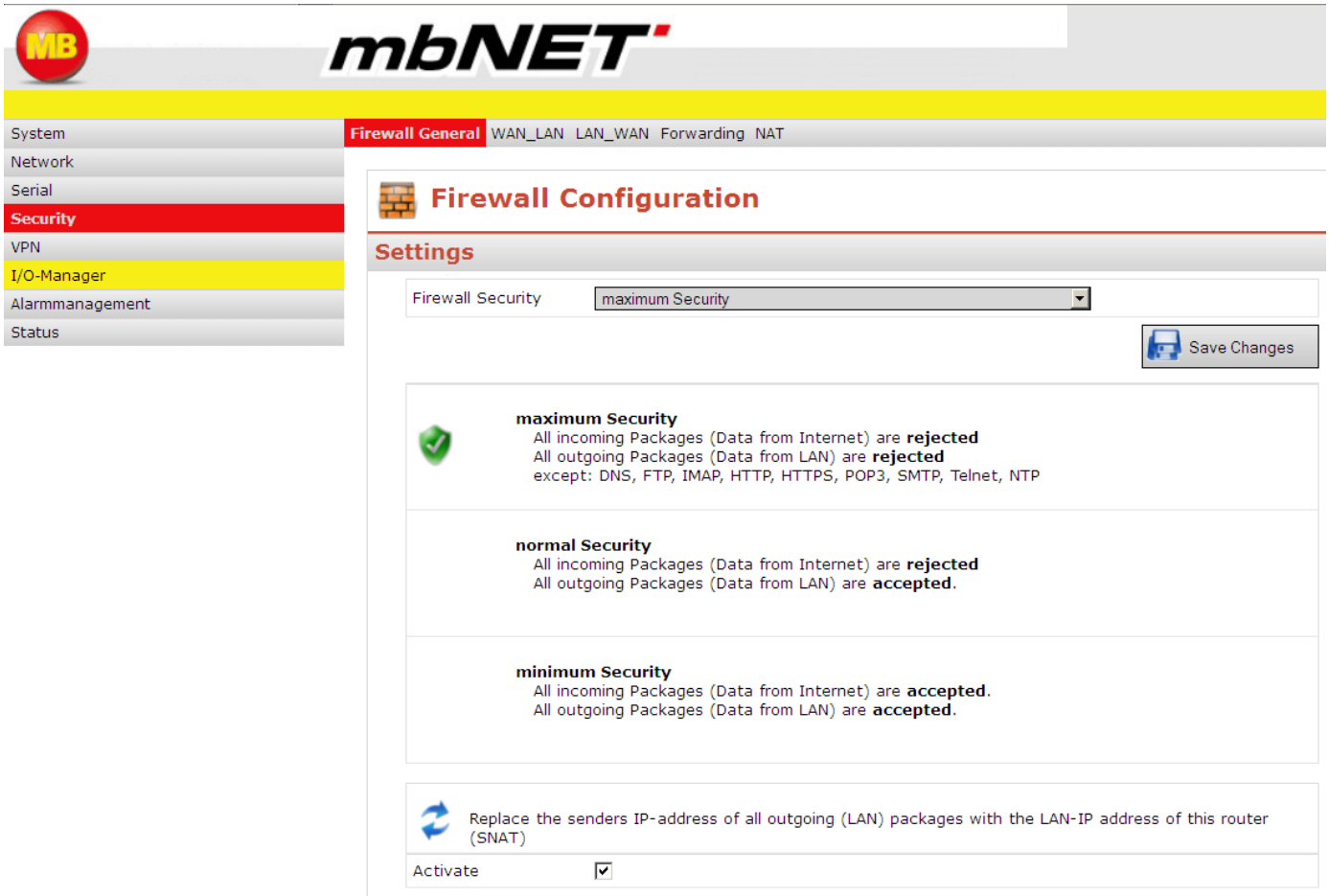
The router settings for this must be as shown below.



RFC1006 can be operated in parallel with this.

15. Security settings

15.1 General



The industrial router has an integrated firewall to protect against third-party and unauthorized access and connection attempts. Incoming and outgoing data traffic is checked, logged and allowed or denied via this firewall.

The firewall can generally be configured with one of the following three settings:

- **maximum Security**
  With this setting, rules for allowing data traffic must be configured accordingly. Both incoming and outgoing data traffic is denied.
  For accessing the web interface (from outside the network), the **TCP protocol** and the **destination port 80** must be entered and enabled in the **WAN >LAN** rules. If, however, you start a VPN connection, access is accordingly allowed for the data packets from the VPN tunnel.
- **normal Security**
  With this setting, incoming data traffic (data from the Internet) is denied while outgoing data traffic is allowed.
- **minimum Security**
  With this setting, all incoming and outgoing data traffic is allowed.

The 'minimum Security' option should only be temporarily set for test purposes since it allows all data traffic from inside to outside the network as well as access from outside the network. This setting threatens the integrity of your mbNET and the connected devices.

SNAT

This function transparently passes on the incoming data traffic from Internet or VPN connections to the LAN. In other words, all data packets going to the LAN are assigned the IP address of the router as the sender address. This means that none of the LAN subscribers need the router as a "gateway". This is a considerable advantage when integrating remote maintenance into existing network structures as it means that these structures do not need to be changed.

Security settings (continued)

15.2 WAN>LAN

This setting governs the incoming data traffic, i.e. the following settings only apply to data traffic arriving from outside the network.

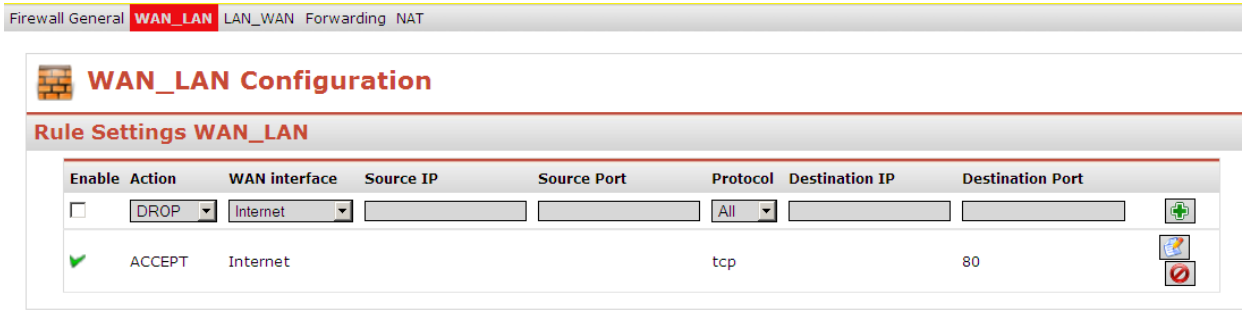


Figure 154

"WAN" is always the currently active interface with the Internet as far as the mbNET firewall is concerned. The following rule is determined by the setting under "Network – Internet":

Internet Connection: Internet via WAN (external router, fixed line)

The WAN Ethernet connection is the interface with the Internet here. The firewall therefore checks the data traffic from the WAN Ethernet to the LAN Ethernet.

Internet Connection: Internet via Modem

The modem is the interface with the Internet here. The firewall therefore checks the data traffic from the modem to the LAN Ethernet. All data traffic on the WAN Ethernet interface is denied with this setting.

Internet Connection: Internet via WAN

The "DSL data traffic" via the WAN Ethernet is the interface with the Internet here. The firewall therefore checks the data traffic from the DSL modem to the LAN Ethernet. All other data traffic on the WAN Ethernet interface is denied with this setting.

In the case of devices with a WAN Ethernet interface, this can be explicitly specified as the firewall interface under the "WAN interface" drop-down field.

Label	Description
Enable	Check the box by clicking it to enable the subsequent settings after they are saved.
Action	The following options are available for selection: **Drop**: If this option is selected, it means that no data packets can pass and the packets are also deleted immediately. The sender is not notified about the whereabouts of the data packets. **Reject**: If this option is selected, the data packets are rejected. The sender is notified that the data packets have been rejected. **Accept**: If this option is selected, the data packets can pass.
WAN interface	This setting defines the WAN interface to which the rule is to be applied. "Internet" or "WAN Ethernet" can be selected.
Source IP	Here, enter the IP for whose incoming data packets one of the set actions is to be executed. If you leave the field blank, the set action applies to all IP addresses.
Source Port	Enter the port via which the data packets arrive here.
Protocol	The following options are available for selection: **All**: The set rule applies to all protocols. **tcp**: The set rule only applies to the TCP protocol. **udp**: The set rule only applies to the UDP protocol. **icmp**: The set rule only applies to the ICMP protocol.
Destination IP	Enter the IP to which the data packets are to be forwarded here.
Destination Port	Enter the port via which the data packets are forwarded here.
	Edits the settings in the current line.
	Deletes entries in the current line.
	Accepts a new rule.
	Temporarily saves the created rule.
	Changes the order of the created rules.

15.3 LAN>WAN

This setting governs the outgoing data traffic, i.e. the following settings only apply to outgoing data traffic.

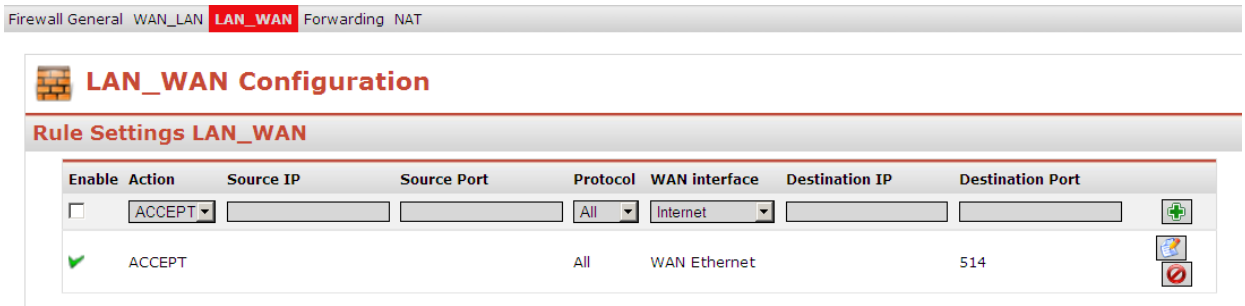

Firewall General WAN_LAN LAN_WAN Forwarding NAT
LAN_WAN Configuration
Rule Settings LAN_WAN
Enable Action Source IP Source Port Protocol WAN interface Destination IP Destination Port
ACCEPT All Internet
ACCEPT All WAN Ethernet 514

Figure 155

Label	Description
Enable	Check the box by clicking it to enable the subsequent settings after they are saved.
Action	The following options are available for selection: **Drop**: If this option is selected, it means that no data packets can pass. The sender is not notified about the whereabouts of the data packets. **Reject**: If this option is selected, the data packets are rejected. The sender is notified that the data packets have been rejected. **Accept**: If this option is selected, the data packets can pass.
Source IP	Enter the IP of a computer from which data packets are sent to the Internet here. If you leave the field blank, the set action applies to all IP addresses.
Source Port	Enter the port via which the data packets go to the Internet here.
Protocol	The following options are available for selection: **All**: The set rule applies to all protocols. **tcp**: The set rule only applies to the TCP protocol. **udp**: The set rule only applies to the UDP protocol. **icmp**: The set rule only applies to the ICMP protocol (ping).
WAN interface	This setting defines the WAN interface to which the rule is to be applied. "Internet" or "WAN Ethernet" can be selected.
Destination IP	Enter the destination address of the data packets on the Internet here.
Destination Port	Enter the port via which the data packets are sent to the destination IP here.
	Edits the settings in the current line.
	Deletes entries in the current line.
	Accepts the new rule and temporarily stores it.
	Temporarily saves the created rule.
	Changes the order of the created rules.

Security settings (continued)

15.4 Forwarding

This setting forwards requests from specific IP addresses and ports to defined IP addresses and ports.

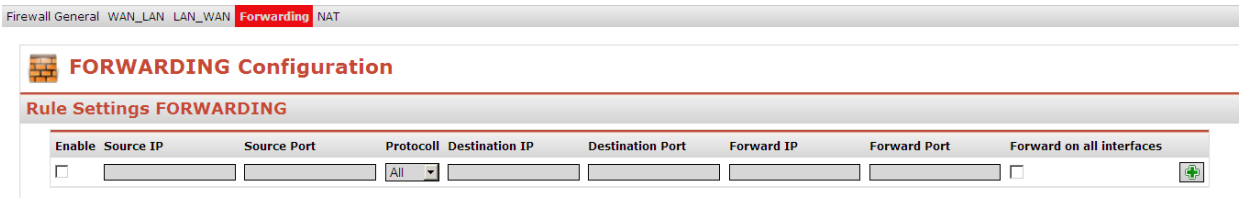

Firewall General WAN_LAN LAN_WAN Forwarding NAT
FORWARDING Configuration
Rule Settings FORWARDING
Enable Source IP Source Port Protocoll Destination IP Destination Port Forward IP Forward Port Forward on all interfaces
All

Figure 156

Label	Description
Enable	Check the box by clicking it to enable the subsequent settings after they are saved.
Source IP	You can enter the IP from which data packets are received here. If an entry is made here, only packets from this one address are forwarded.
Source Port	You can specify the port via which the data packets arrive here. If an entry is made here, only packets specifically sent via this port are forwarded.
Protocol	The following protocols are available for selection: **All**: The set rule applies to all protocols. **tcp**: The set rule only applies to the TCP protocol. **udp**: The set rule only applies to the UDP protocol.
Destination IP	Enter the IP to which the data packets were originally to be sent here.
Destination Port	Specify the port via which the data packets are sent to the destination IP here.
Forward IP	Enter the IP to which the data packets are actually to be sent here.
Forward Port	Specify the port via which the data packets are actually forwarded here.
Forward on all interfaces	The "FORWARDING" setting is applied to all connections, i.e. even incoming VPN connections. If this option is not set, the setting only applies to incoming packet from the Internet, but not a VPN connection via the Internet.
	Accepts the new settings and temporarily stores them.

15.5 NAT

This setting enables two networks in the same address range to be connected. If, for example, a network with the address 192.168.0.0/24 is to be connected to a network with the same address, this is only possible if one of the two networks is assigned another address. NAT technology is an easy way of achieving this since only the real network address (LAN address) and the substitute address (NAT network address) are required. The NAT algorithm makes sure that the addresses in the data packets are only substituted in communications between these two networks. This means that you do not have to adapt your entire network addressing scheme.

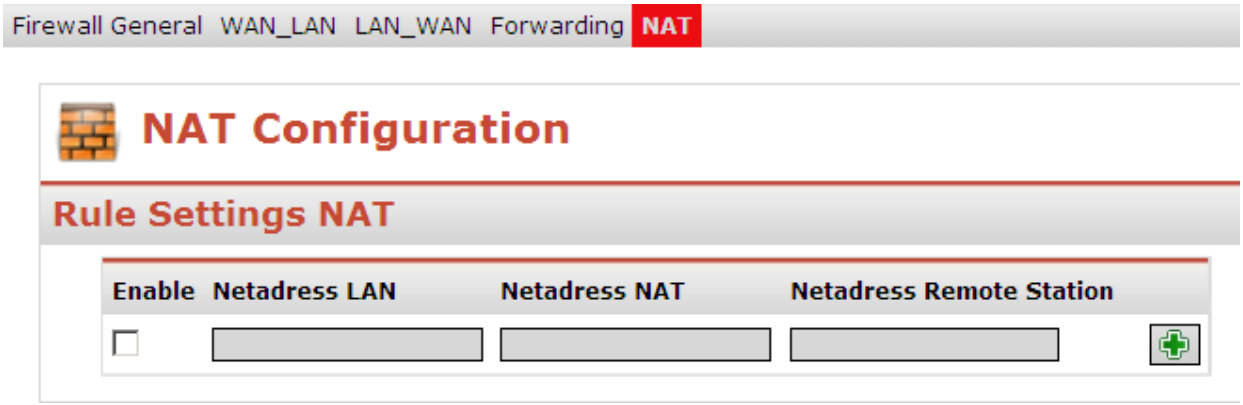


Figure 157

Label	Description
Enable	Check the box by clicking it to enable the subsequent settings after they are saved.
Netaddress LAN	Enter the real address of the network here (e.g.192.168.0.0/24). **Please note that the IP address must be entered in CIDR notation.**
Netaddress NAT	Enter the translated address of your network here (e.g. 192.168.1.0/24).**Please note that the IP address must be entered in CIDR notation.**
Netaddress Remote Station	Enter the address of the network to which the translated packets are to be routed here. If the remote station also uses address translation, the NAT address of the remote station must be entered here.
	Accepts the new settings and temporarily stores them.

16. VPN-IPSec

16.1 Configuring a VPN-IPSec connection with two routers

- ❑ The settings for a VPN connection via the IPSec protocol are described below.
- ❑ From the start page, click **VPN** in the navigation bar on the left and **IPSec** in the navigation bar at the top.
- ❑ Click the button on the right to create an IPSec connection.
- ❑ The following screen appears:

Figure 158

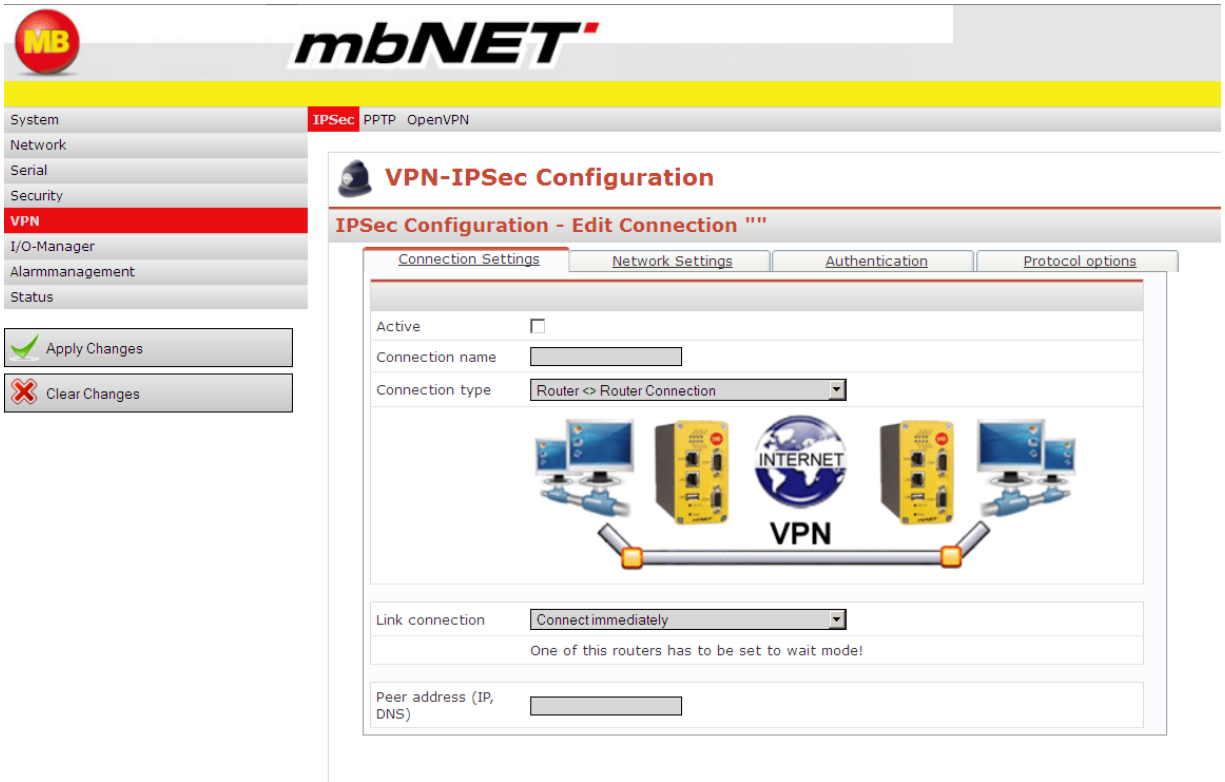


Figure 159

16.1.1 Connection settings

Tab	Label	Description
Connection Settings	**Active**	Check this box to activate the VPN connection.
	Connection name	Enter a name for the connection in the input field.
	Connection type	Select the connection type **Router <> Router Connection** or **Client <> Router Connection** via the drop-down field.
	Link connection **(only with a router-router connection)**	Please note that to communicate with another router, this router must be configured for accessing the Internet and for requests from clients. With a ***router-router connection***, one of the following options for establishing a connection must be selected: **Connect immediately:** A connection is established following a restart or boot routine. **Connect on traffic** The connection with the router or remote network is established in response to requests from the local network. **Wait for incoming Connection** The router on standby is the so-called VPN server. It waits for incoming connections.
	Peer address (IP, DNS) **(only with a router-router connection)**	The appropriate peer address must be specified on the router responsible for the outgoing connections. This can be an IP address or even the DNS name under which the remote router can be reached.

16.1.2 Network Settings

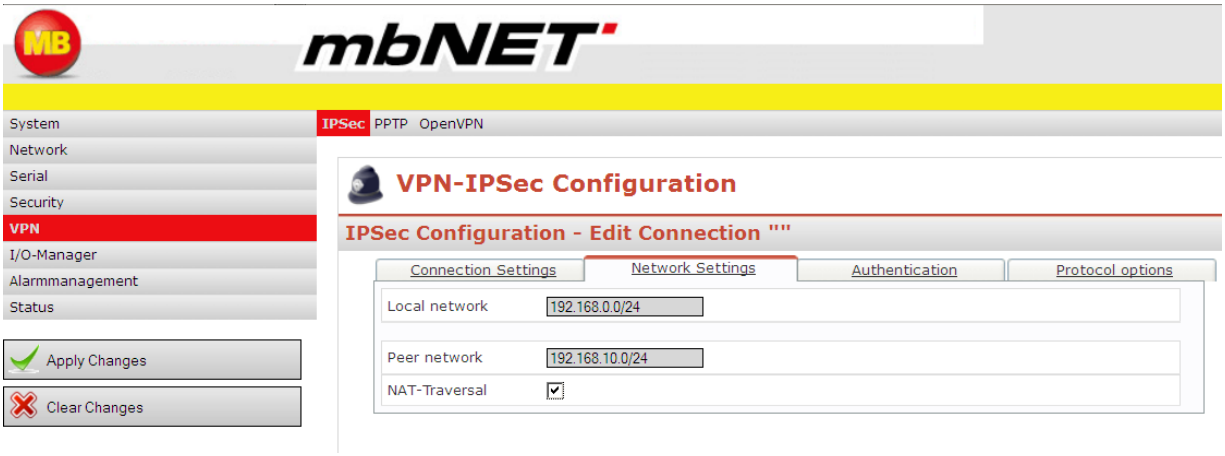


Figure 160

16.1.3 Authentication

Tab	Label	Description
Network Settings	**Local network**	Enter the address range of the local network in CIDR notation here. E.g. 192.168.0.0/24
	Peer network (only with a router-router connection)	Enter the address range of the local network in CIDR notation here. E.g. 192.168.10.0/24
	NAT-Traversal (only with a router-router connection)	This setting is necessary if the VPN connection is established via the Internet and natted between the LAN and WAN (NAT: Network Address Translation). This setting is generally enabled.
	Permitted network for the client (only with a client-router connection)	Set the network accessed by the client here. It must be entered in CIDR notation.
	Client has a fixed IP address or name (only with a client-router connection)	If the client has a fixed static address, this address must be entered in this input field.
	Win2000 / XP Client (L2TP) (only with a client-router connection)	Set whether the client is a PC running the Windows 2000 or XP operating system here.

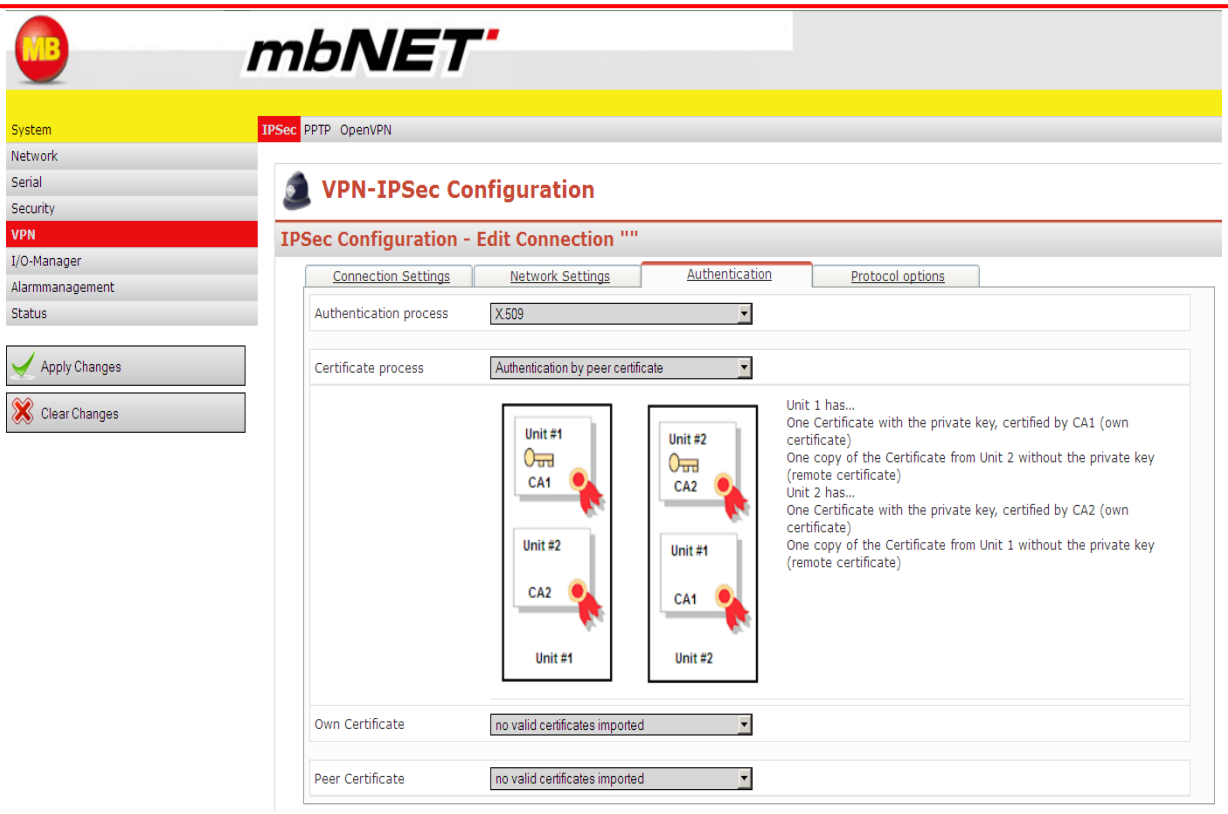
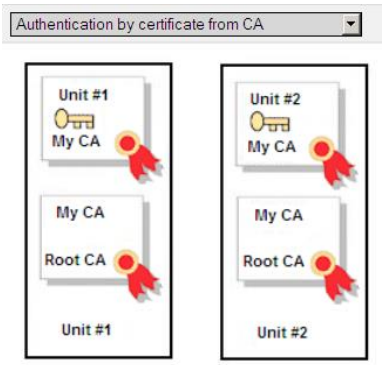
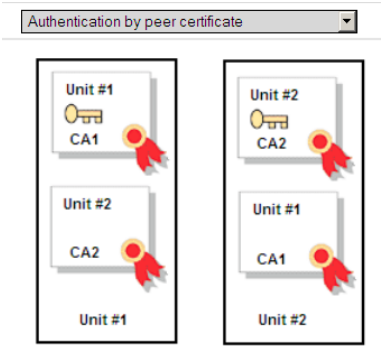


Figure 161

Authentication (continued)

Tab	Description

Authentication		Select the **Authentication process** via the drop-down field. **PSK:** Both keys must be known before data can be exchanged between the client and router. The longer the keys, the more secure the connection. **Only one** key can be specified. Even if there are several PSK connections entered, the key for the **FIRST** connection is universally valid. **Local ID:** Assign a name for your router here. This name must be communicated to the peer**.** **Peer ID:** Enter the name of the peer here. **X.509:** **You can choose between two authentication processes via the drop-down field:** **Authentication by certificate from CA:** The root certificate (certificate authority, CA for short) and a personal certificate including key (.p12 file) must be imported into the router for this. (See the section System – Certificates). The remote station must have the same root certificate and a certificate signed by the CA including key. **Authentication by peer certificate:** The certificates can be signed by different CAs. A personal certificate+key (.p12 file) must be imported into each router. Each router must also have a copy of the respective peer certificate, naturally WITH-
		

		OUT the key (.crt file). **Own Certificate:** Select the router's personal certificate via the drop-down field. **Local ID:** This ID is normally assigned by the certificate. This field can be left blank. **Peer Certificate:** Select the peer certificate here. **Peer ID:** This ID can only be assigned by the certificate if **Authentication by peer certificate** was selected. The field can be left blank in this case. If, however, **Authentication by certificate from CA** was selected, you must specify the peer ID (**in case you want to establish the connection**). This ID is selected when the certificate is created (see the section Creating certificates and revocation lists using XCA under the tab Subject). It is the certificate subject and must be entered as follows: */C=country/ST=state/L=city/O=organization/OU=department/* *CN=certificate_name/E=email_address* If some fields on the **Subject** tab were left blank when the certificate was created, the corresponding entries must be omitted (cf. the section Creating certificates and revocation lists using XCA). **Peer Certificate:** Only if **Authentication by peer certificate** was selected. Select the corresponding certificate via the drop-down field.

16.1.4 **Protocol options**

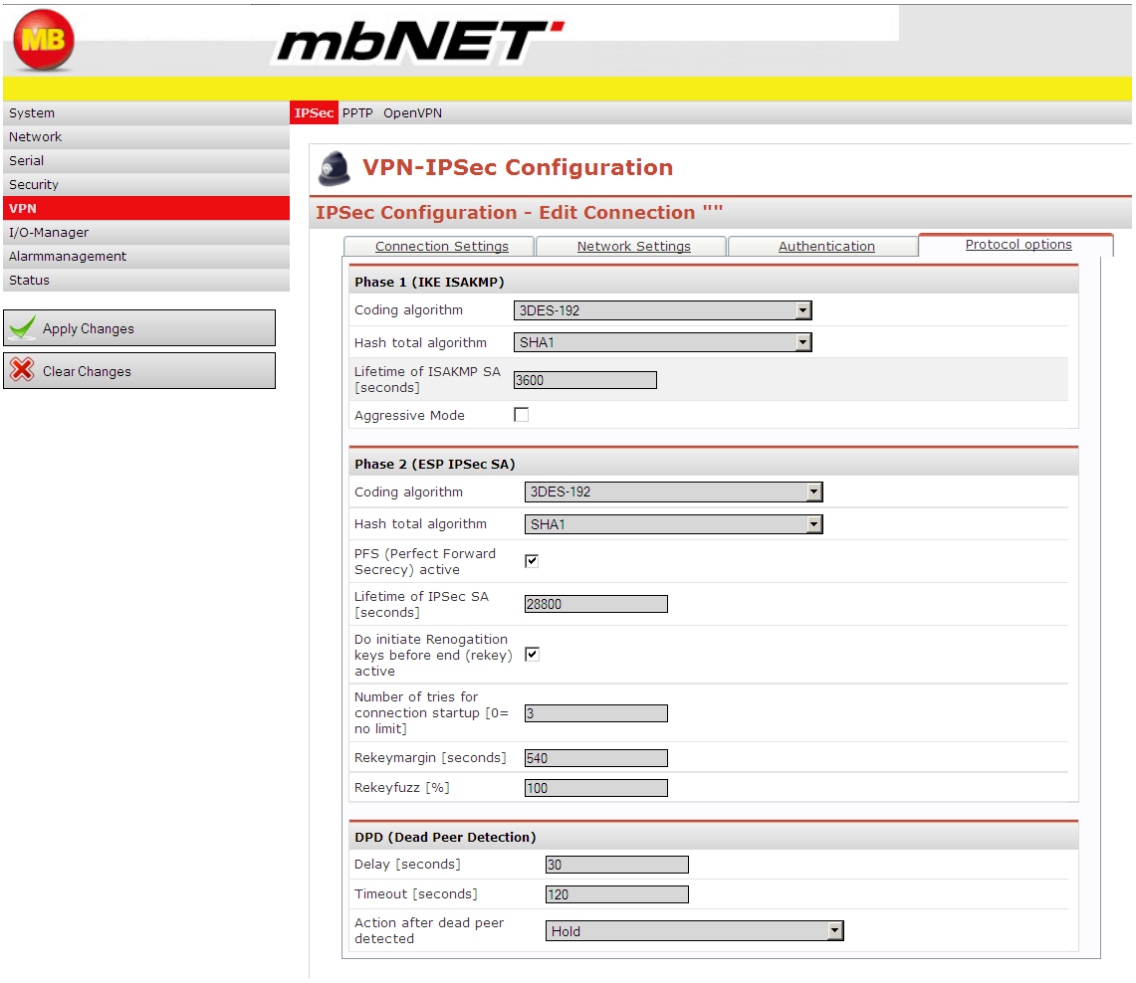


Figure 162

Label	Description
Protocol options	You select the coding algorithms, hash total algorithms, etc. used during the various phases on this tab.
	PFS: This setting is only supported for the router-router connection. PFS must be disabled if you want to set up a client-router connection.

16.1.5 L2TP Server Configuration

The L2TP server can be used for VPN-IPSec communication between the industrial router and a Windows client. The only setting required here is a freely selectable local IP address. The addressees for the clients should be from the same network (the start and end of the range are set under the IP address field). The L2TP server then works in a similar way to a DHCP server and can automatically assign the addresses from the set range to the clients dialing in.

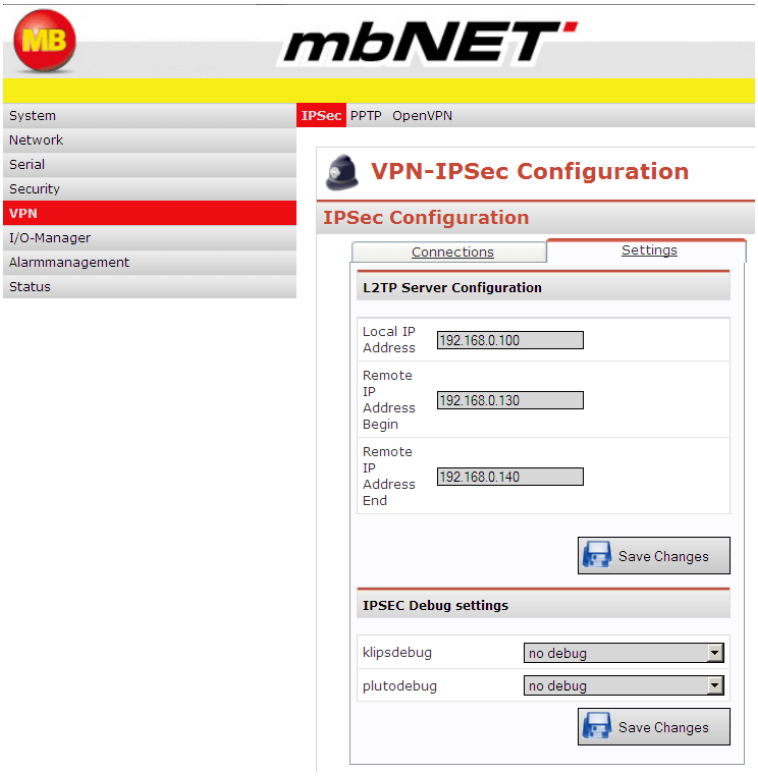


Figure 163

Label	Description
Local IP Address	The name or IP address to be assigned to the server during communication with the Window client must be entered here. In the example this is 192.168.0.100
Remote IP Address Begin **Remote IP Address End**	Assignment of client IP addresses. The address range from which remote clients are assigned their IP address can be set here. In the example this is 192.168.0.130 to 192.168.0.140

17. VPN-PPTP

17.1 Server settings

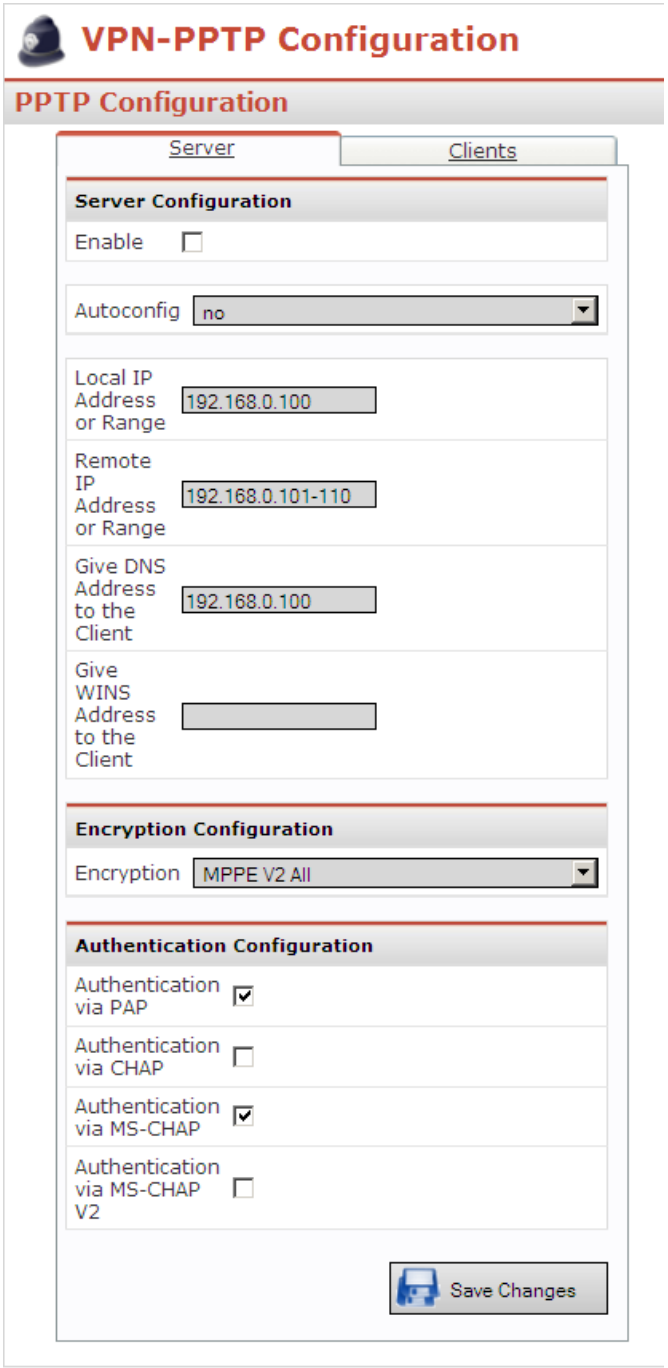


Figure 164

Label	Description
Enable	Check this box by clicking it if the industrial router is to be enabled as a VPN server.
Autoconfig	The local address of the mbNET will be used if you select "yes" here. Read on if you selected "no".

Local IP Address or Range **Remote IP Address or Range**	A local and remote address (start and end point of the tunnel) is needed to set up a transmission channel. You can enter either an individual IP address or an entire range here. The remote range specification determines the maximum number of clients that can dial in simultaneously. **Example:** Local IP address: 192.168.0.104 Remote IP address: 192.168.0.160 The VPN server can be accessed under the IP address 192.168.0.104. Only the client assigned the IP address 192.168.0.160 (by the server) can log in to the server. Example: Local IP address: 192.168.0.104 Remote IP address: 192.168.0.160-170 The connected clients (max. 10) that can dial in simultaneously are assigned the IP addresses 192.168.0.160 to 192.168.0.170 by the server 192.168.0.104.

VPN-PPTP (continued)

Label	Description
Give DNS Address to the Client	Here, enter the DNS server address that is assigned to a client dialed into the router in order to resolve computer names into IP addresses and vice versa.
Give WINS Address to the Client	Here, enter the WINS server address for NetBIOS name resolution that is assigned to a client dialed into the router.
Encryption	Select the encryption method here via the drop-down field: None: No encryption MPPE V2 40:40-bit encryption MPPE V2 128: 128-bit encryption MPPE V2 All: All encryption methods
Authentication via PAP	Select the authentication method here. The client keeps sending the username/password combination to the host until it accepts or rejects authentication of the client.
Authentication via CHAP	Select the authentication method here. This authentication method is controlled by the host. When a client dials in, it is prompted by the host to authenticate itself. The client sends username/password using MD5 encryption. The authentication is accepted if the user data sent matches the data on the host. If not, it is rejected. If the authentication is accepted, the user data is periodically checked during the connection.
Authentication via MS-CHAP	Proprietary authentication protocol developed by Microsoft.
Authentication via MS-CHAP V2	Proprietary authentication protocol developed by Microsoft.

17.2 Client setting

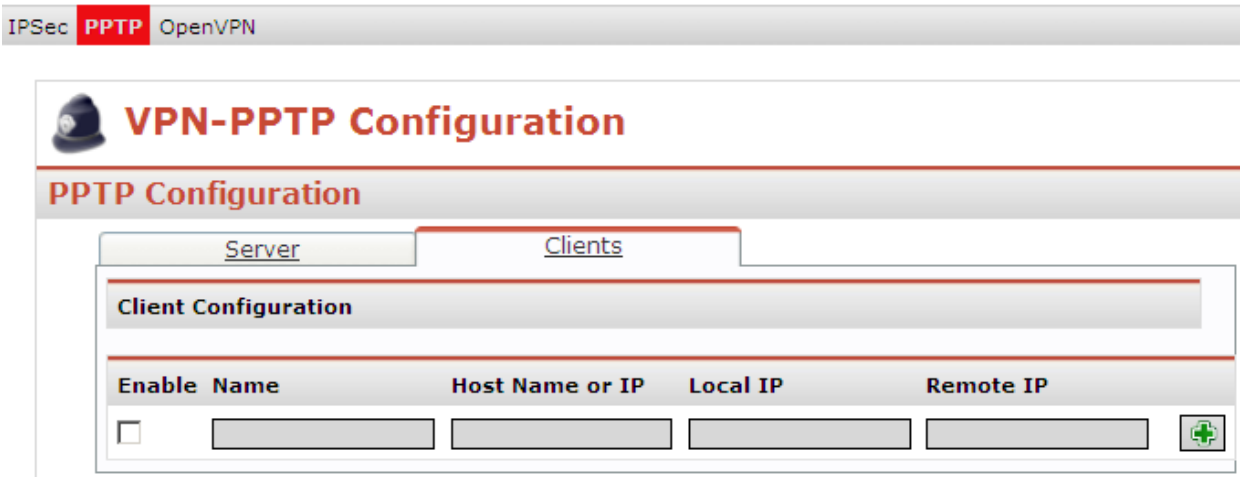


Figure 165

Label	Description
Enable	Check this box by clicking it if the industrial router is to be enabled as a VPN client.
Name	Enter a name for the client here.
Host Name or IP	Enter the name or IP address under which the client accesses the server here. Example 123456789@mbNET.mymbnet.biz or 80.187.33.55
Local IP	**This entry is optional.** If the server is not configured to assign an IP address to the client, the client can request the IP address entered here. The settings are generally made on the VPN server. This setting is for compatibility with other routers.
Remote IP	Enter the network address of the server in CIDR notation here (e.g. 192.168.0.0/24) in order to have a route into the server network.

18. VPN – OpenVPN

18.1 Basics about OpenVPN

-OpenVPN basically works with two tunnel IP addresses, i.e. each connection has two IP addresses via which the data traffic is processed.
- Depending on the authentication method, OpenVPN either works in point-to-point mode (with static key or no authentication) or in server/client mode (with X.509 certificates).
- OpenVPN can use three different authentication methods:
  - **None**: No certificate or key is needed. Used primarily for testing the connection. The tunnel data is also **NOT** encrypted.
  - **Static key**: A 1024-bit key as required by each peer is generated for the connection. Similar to the password.
  - **Certificates, X.509**: The following certificate variants are distinguished:
    - Each subscriber needs the same root CA and a personal certificate signed by the root CA.
    - Like 1, but with additional username/password verification.
    - Like 2, but without a personal certificate. In other words, subscribers only need a root CA and username/password.
- OpenVPN can use an http proxy server as the outgoing connection. This is important for integration into existing corporate networks with an Internet connection.

- The transmission protocol setting (UDP or TCP) can be freely selected with OpenVPN. The same applies to the port numbers to be used for the transmission protocol.

❑ The settings for various OpenVPN connection scenarios are described below.

❑ From the start page, click **VPN** in the navigation bar on the left and **OpenVPN** in the navigation bar at the top.

- Click the button on the right to create an OpenVPN connection.

Figure 166

18.2 Connection scenarios

18.2.1 Client – router

- **The connection wizard** helps you to configure your connections quickly and easily. To access the wizard, click the "Wizards" link in the top right of the web interface. If you have disabled the autolaunch function for the wizard, click the Start button for the wizard for VPN connections.

  Please note that you must first select "OpenVPN" in the menu under the Start button for the VPN wizard. You must then click "Save Changes" and "Apply Changes" so that you can configure a connection with OpenVPN.

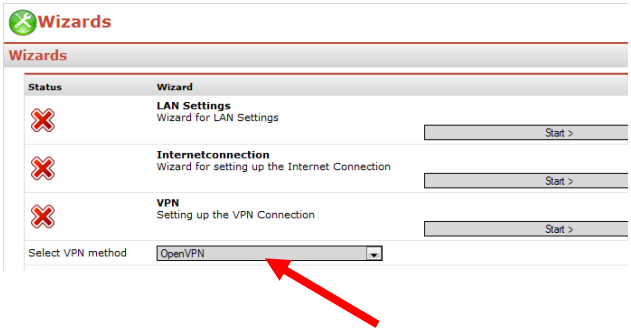


Figure 167

- Select the option "Connection between Networkclient and mbNet".

- Next select the static key. If you have not yet created a static key, you can use the key created by mbNET. Click "Next".

- Clicking "Next" completes the configuration of the connection. Click "Finish" to apply your settings. You must have OpenVPN installed on your computer to establish a connection. You can find out more about this in section 18.2.1.3 "Configuring an OpenVPN Windows client".

Figure 168

.

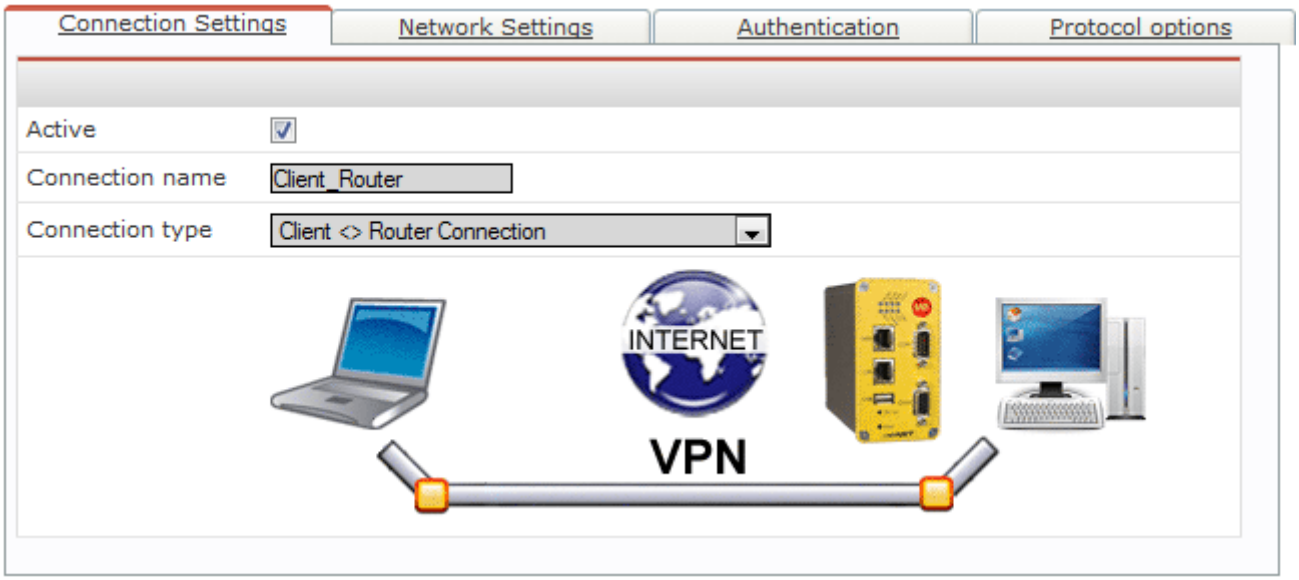


Figure 169

Tab	Label	Description
Connection Settings	**Active**	Check this box to activate the OpenVPN connection.
	Connection name	Enter a name for the connection in the input field.
	Connection type	Select the connection type **Client <> Router Connection** via the drop-down field.

Only one "client to network" connection can be created. Depending on the authentication method, the client receives an IP address from a defined range or each subscriber specifies its requested address.

```
Example:

Client PC                       mbNET
[10.1.0.6]  VPN - TUNNEL        [10.1.0.5] <> ROUTING <> LAN [192.168.0.100]
```

18.2.1.1 No authentication or static key

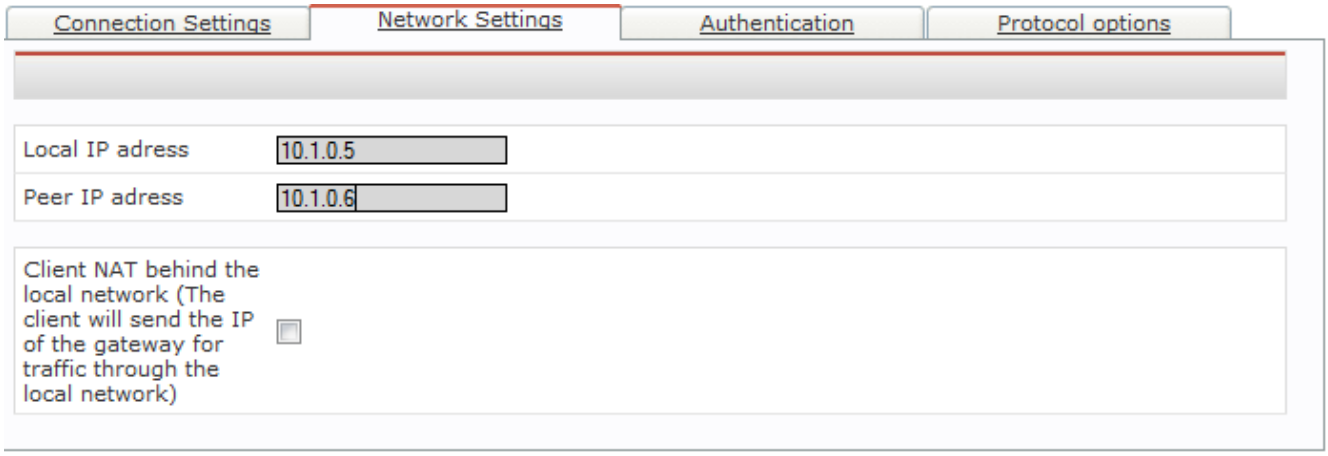

Connection Settings
Network Settings
Authentication
Protocol options
Local IP adress
10.1.0.5
Peer IP adress
10.1.0.6
Client NAT behind the local network (The client will send the IP of the gateway for traffic through the local network)

Figure 170

Tab	Label	Description
Network Settings	**Local IP address**	Enter the IP address of the local VPN tunnel end point here, e.g. 10.1.0.5
	Peer IP address	Enter the IP address of the peer VPN tunnel end point here, e.g. 10.1.0.6
	Client NAT behind the local network (The client will send the IP of the gateway for traffic through the local network)	All packets coming into the LAN receive the sender IP address of the mbNET. Although this means that it is then no longer possible to distinguish between senders in the LAN, the LAN subscribers do NOT have to have the mbNET entered as a gateway.

With authentication without certificates, only one IP channel (local IP address and peer IP address) can be specified per connection entry.

With manual configuration of the VPN client, the setting "Local IP address" and "Peer IP address" must be reversed accordingly on the client.

18.2.1.2 Authentication with certificates

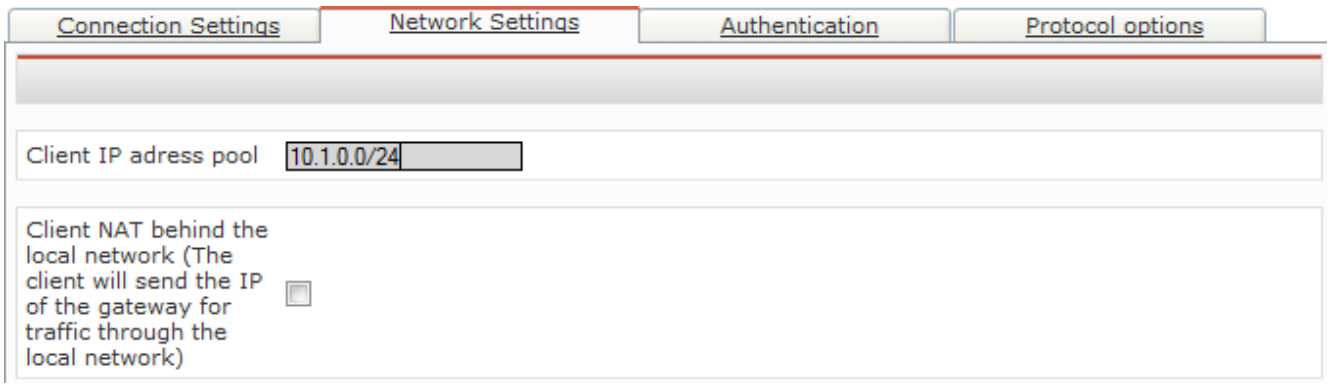

Connection Settings
Network Settings
Authentication
Protocol options
Client IP adress pool
10.1.0.0/24
Client NAT behind the local network (The client will send the IP of the gateway for traffic through the local network)

Figure 171

Tab	Label	Description
Network Settings	**Client IP address pool**	With authentication with certificates, multiple clients can dial into the server simultaneously and are automatically assigned an IP address from the "Client IP address pool". Enter the address range in CIDR notation. E.g. 10.1.0.0/24 (corresponds to the subnet mask: 255.255.255.0).
	Client NAT behind the local network (The client will send the IP of the gateway for traffic through the local network)	The option "Client NAT behind the local network (The client will send the IP of the gateway for traffic through the local network)" assigns all packets coming into the LAN the sender IP address of the mbNET. Although this means that it is then no longer possible to distinguish between senders in the LAN, the LAN subscribers do NOT have to have the mbNET entered as a gateway. NOTE - this can become confusing with multiple clients.

No network settings need to be made on the client side. The server automatically passes all the information to the client in this mode.

18.2.1.3 **Configuring an OpenVPN Windows client**

To be able to use the OpenVPN Windows client, it must first be installed on the computer. The installation routine can be downloaded from
http://openvpn.net/index.php/open-source/downloads.html .
The corresponding client setting can be downloaded from the mbNET via the "Download" link (see arrow). Save this file in the "config" folder of OpenVPN.

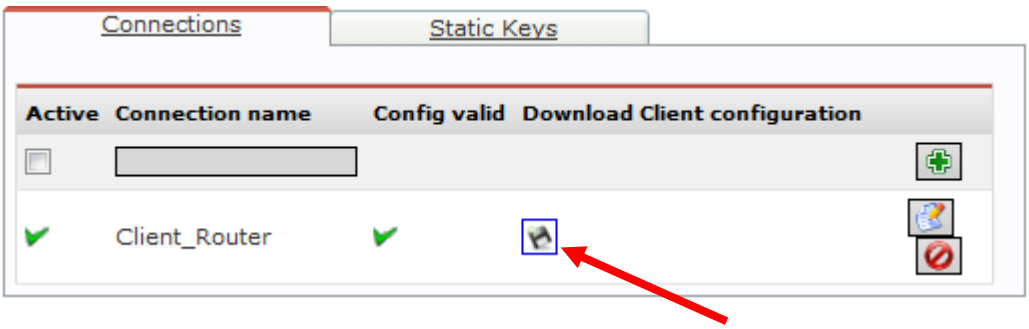


Figure 172

With manual configuration of the VPN client, the setting "Local IP address" and "Peer IP address" must be reversed accordingly on the client.

The downloaded file corresponds to the settings for OpenVPN for Windows. Open the settings file using a text editor to make the additional settings:

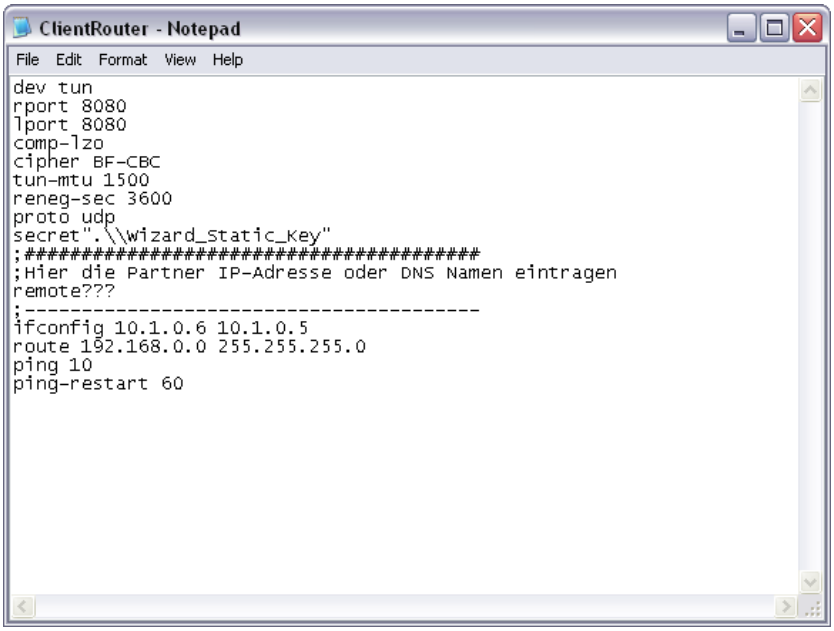


Figure 173

18.2.1.3.1 No authentication

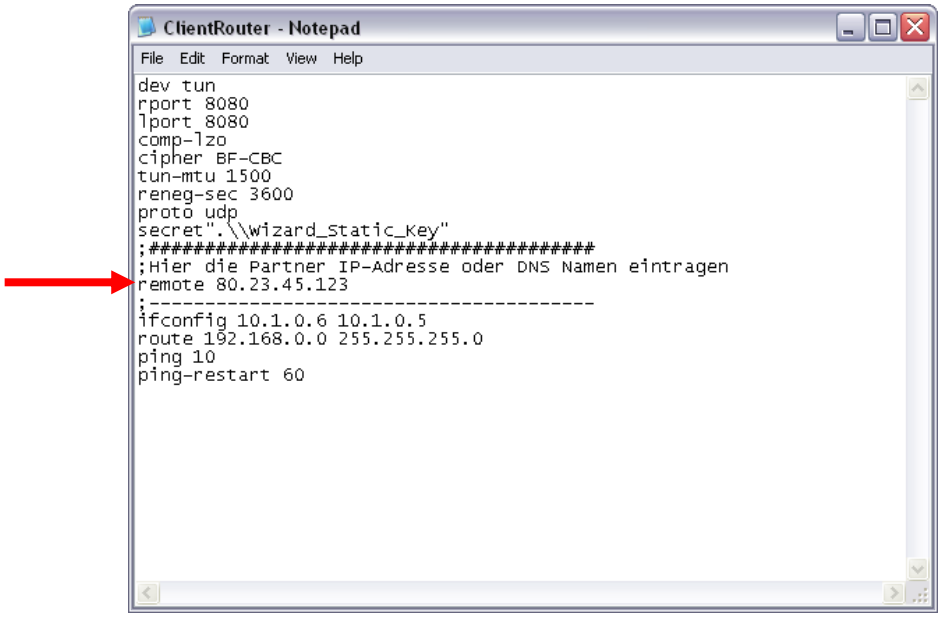


Figure 174

To be able to establish an OpenVPN connection with your mbNET without encryption, you just need to delete the `????` after "`remote`". Next enter the public IP address of the mbNET
(the address accessible via the Internet) or use MB Connect Line's DynDNS service. You must then enter the name specified under **Network DynDNS**.
(E.g. `remote 0123456789.mbNET.mymbnet.biz`)

18.2.1.3.2 Authenticating a Windows client with static key

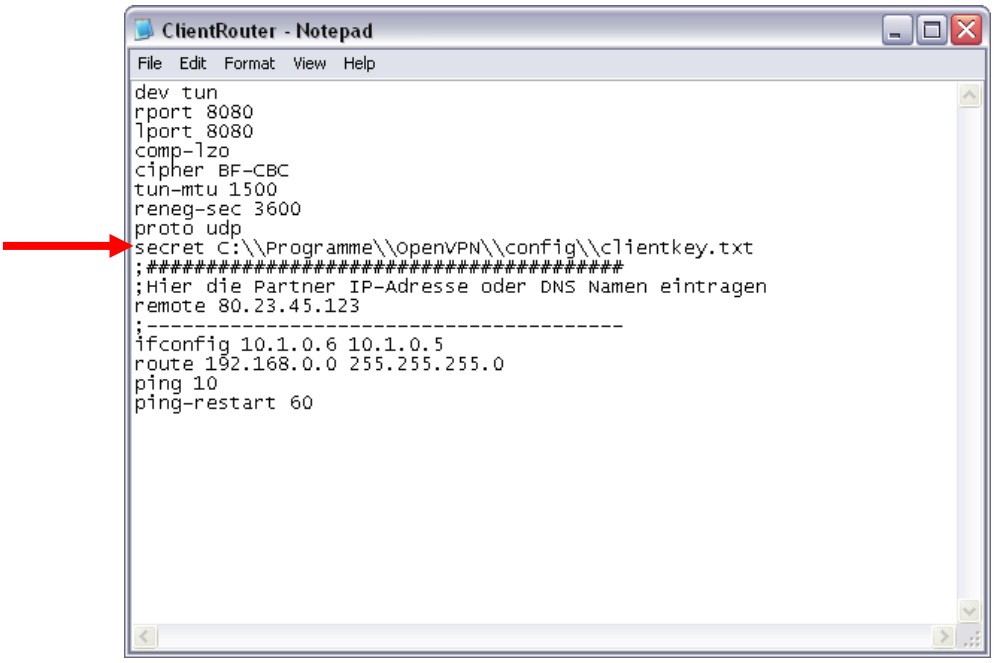


Figure 175

If you have decided on the method with the static key, you must make a private (secret) entry in addition to entering the IP address (see arrow). Note that you must always use **two backslashes** in the path name.

Authenticating a Windows client with certificates

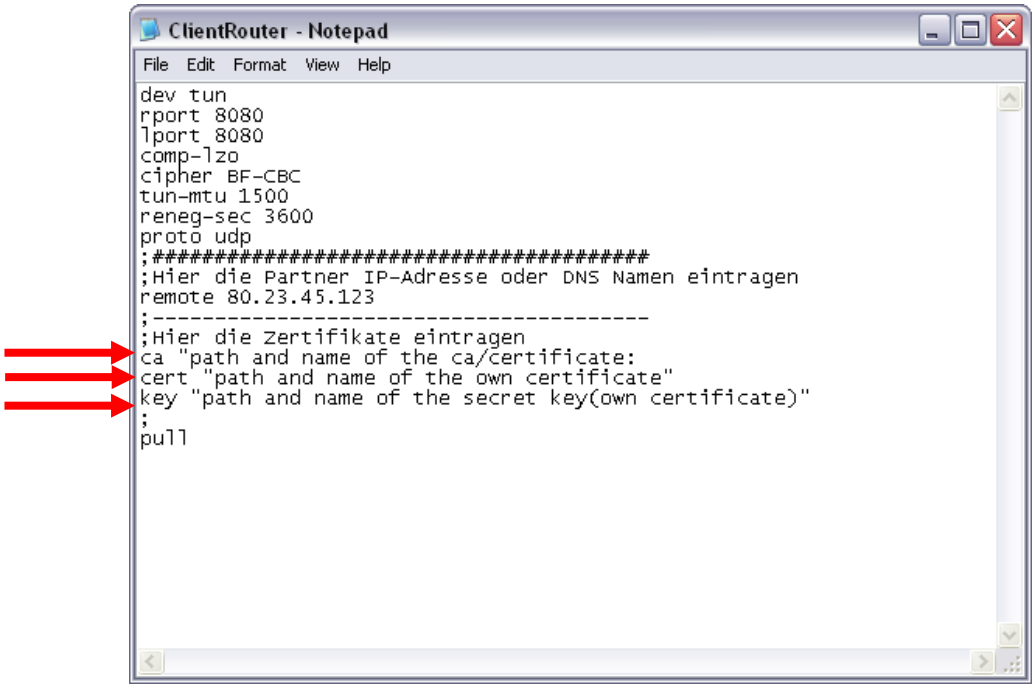


Figure 176

Change the indicated options as appropriate to your circumstances. Note that you must always use **two backslashes** in the path name and that you need the key of your personal certificate for the directive "key".

18.2.1.3.3 Starting the OpenVPN connection

After completing the configuration, you can right-click the .ovpn file or start the connection via the graphical interface in the toolbar as shown below.

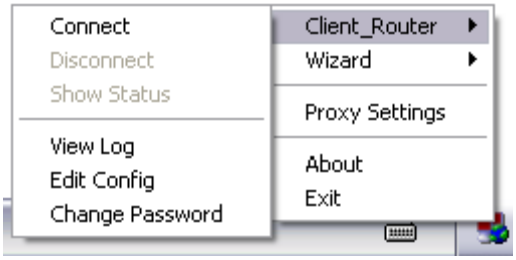


Figure 177

18.2.2 Router – router

- **<u>Using the connection wizard:</u>** Click the "Wizards" link in the top right of the web interface. Then click the Start button for the wizard for VPN connections, followed by "Next".
- Select "Connection between 2 Networks" (Figure 158).
- Select the VPN server in the following window and click "Next".
- You must then specify the local network address and subnet mask of the VPN client (Figure 159).
- Enter the key of your choice in the following window or use the key generated by mbNET.
- Click "Finish" to complete the configuration and accept your settings. Repeat this configuration with the VPN client. This time, however, you must select the VPN client instead of the VPN server.

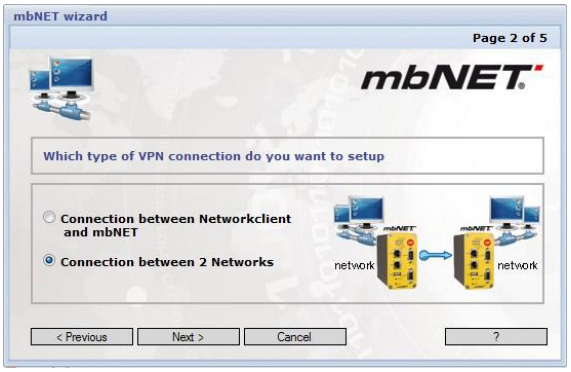


Figure 178

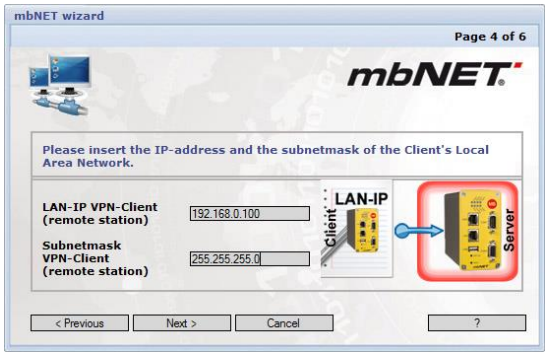


Figure 179

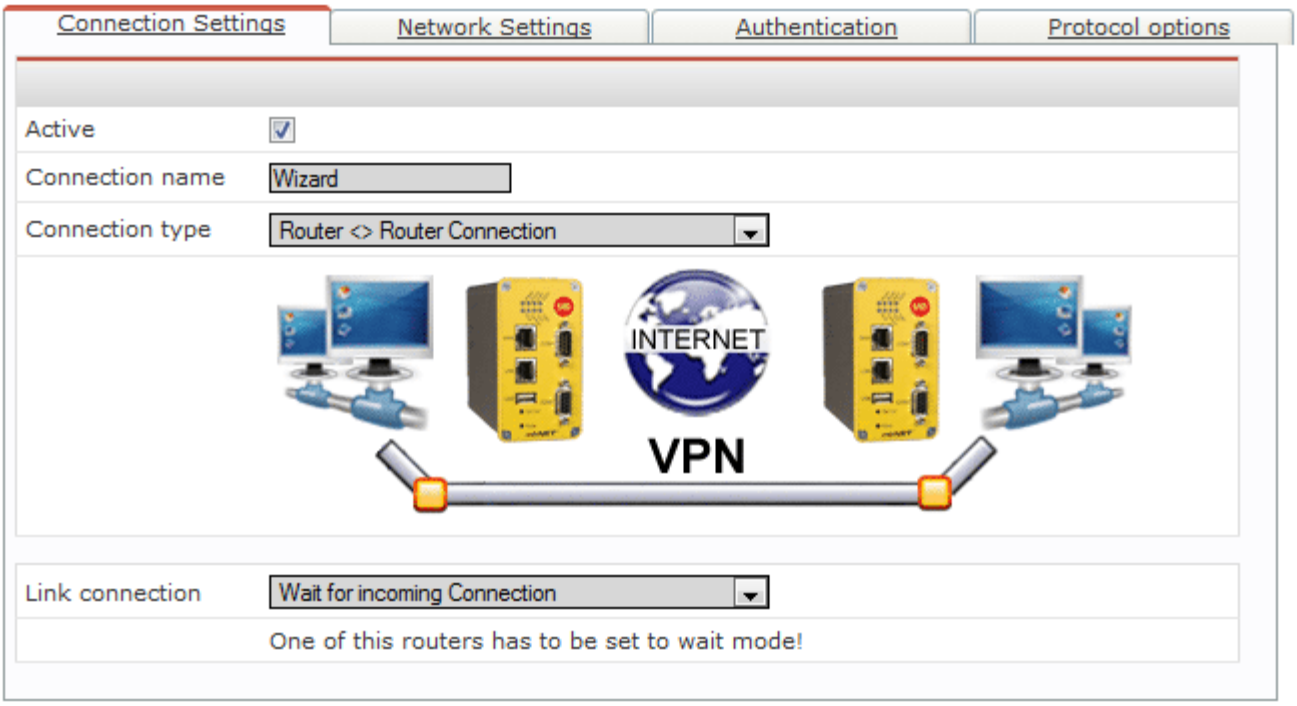


Figure 180

Tab	Label	Description
Connection Settings	**Active**	Check this box to activate the OpenVPN connection.
	Connection name	Enter a name for the connection in the input field.
	Connection type	Select the connection type via the drop-down field.

A "network to network" connection can be created here. Depending on the authentication method, the client receives an IP address from a defined range or each subscriber specifies its requested address.

```
Example:

LAN                    mbNET Client                    mbNET Server LAN
[192.168.99.100]<>ROUTING<>[10.1.0.2] VPN - TUNNEL [10.1.0.1]<>ROUTING<>[192.168.0.100]
```

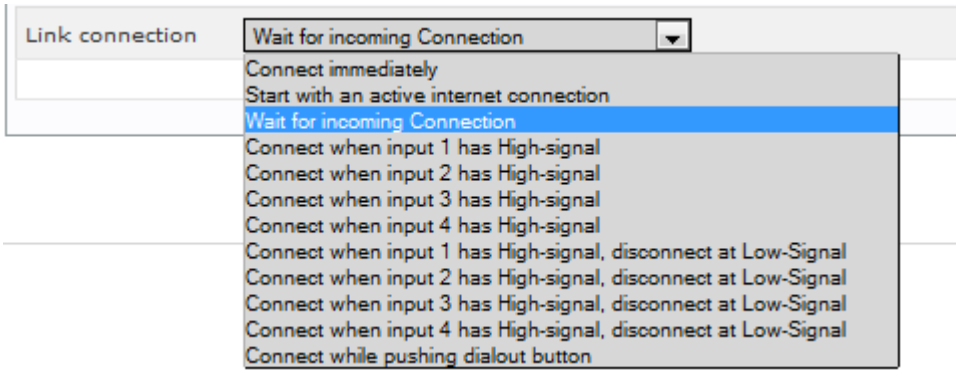

Link connection
Wait for incoming Connection
Connect immediately
Start with an active internet connection
Wait for incoming Connection
Connect when input 1 has High-signal
Connect when input 2 has High-signal
Connect when input 3 has High-signal
Connect when input 4 has High-signal
Connect when input 1 has High-signal, disconnect at Low-Signal
Connect when input 2 has High-signal, disconnect at Low-Signal
Connect when input 3 has High-signal, disconnect at Low-Signal
Connect when input 4 has High-signal, disconnect at Low-Signal
Connect while pushing dialout button

Figure 181

If "Wait for incoming Connection" was selected for the link connection, this is called mbNET in server mode and "Server" in the rest of the documentation.
If "Connect immediately" or "Start with an active internet connection" was selected for the link connection, this is called mbNET in client mode and called "Client" in the rest of the documentation.

18.2.2.1 Server – no authentication or static key

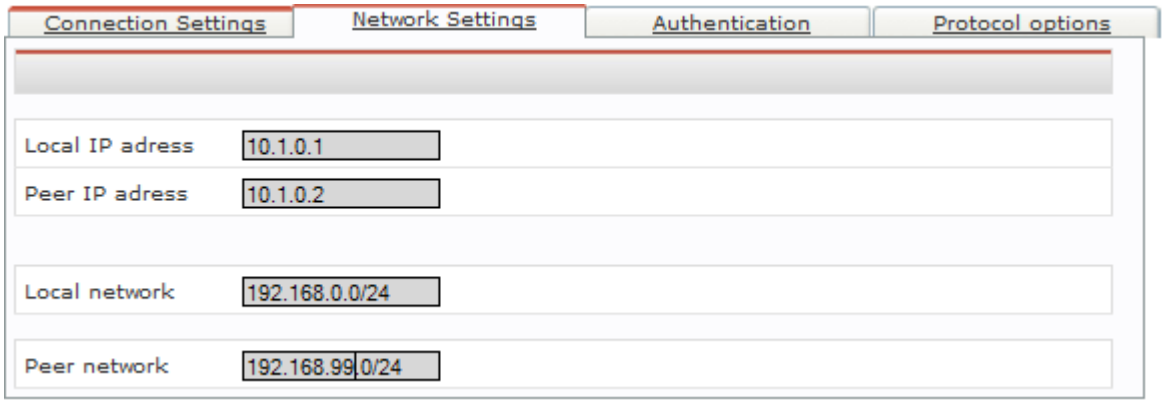


Figure 182

Tab	Label	Description
Network Settings	**Local IP address**	Enter the IP address of the local VPN tunnel end point here, e.g. 10.1.0.1
	Peer IP address	Enter the IP address of the peer VPN tunnel end point here, e.g. 10.1.0.1
	Local network	Enter your network address in CIDR notation here (192.168.0.0/24).
	Peer network	Enter the network address of your peer in CIDR notation here (192.168.99.0/24).

With authentication without certificates, only one IP channel (local IP address and peer IP address) can be specified per connection entry.

With manual configuration of the VPN client, the setting "Local IP address" and "Peer IP address" must be reversed accordingly on the client.

18.2.2.2 Server – authentication with certificates

With authentication with certificates, multiple clients can dial into the server simultaneously and are automatically assigned an IP address from the "Client IP address pool".
There are two different operating modes in server mode with certificates.

18.2.2.2.1 Single client: Only one client can dial in

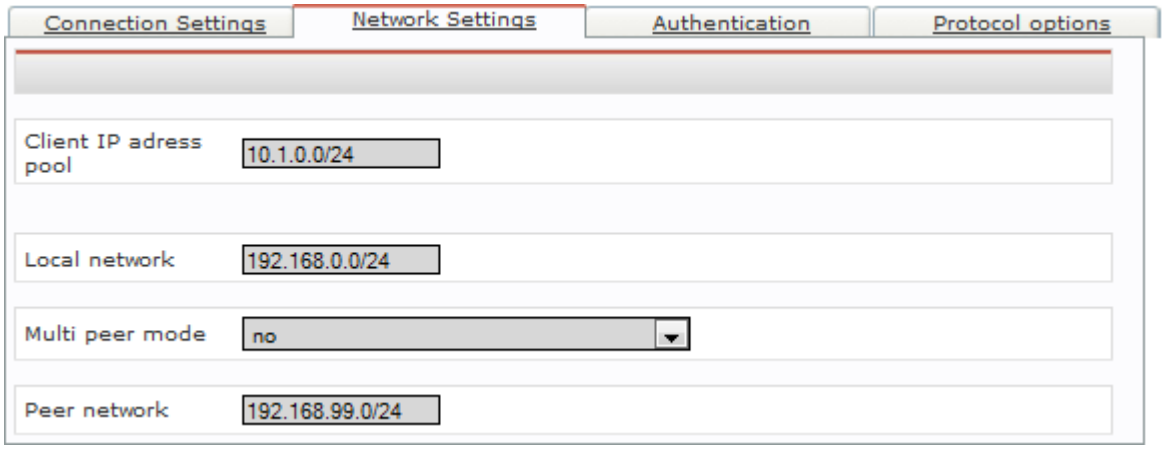


Figure 183

Tab	Label	Description
Network Settings	**Client IP address pool**	With authentication with certificates, multiple different clients can dial into the server (not simultaneously) and are automatically assigned an IP address from the "Client IP address pool". Enter the address range in CIDR notation. E.g. 10.1.0.0/24
	Local network	Enter the address range of the local network in CIDR notation here. E.g. 10.1.0.2/24
	Multiple peers with different network addresses can establish a VPN connection.	"no" selected Each client is assigned the peer network address range, which means that simultaneous client logins make no sense here.
	Peer network	Enter the network address of your peer in CIDR notation here (192.168.99.0/24).

No network setting is needed on the client because it is sent to the client by the server.

The local network and the peer network must be specified. OpenVPN then creates the necessary routing entries using these entries.

18.2.2.2.2 Multi client: Multiple clients can dial in

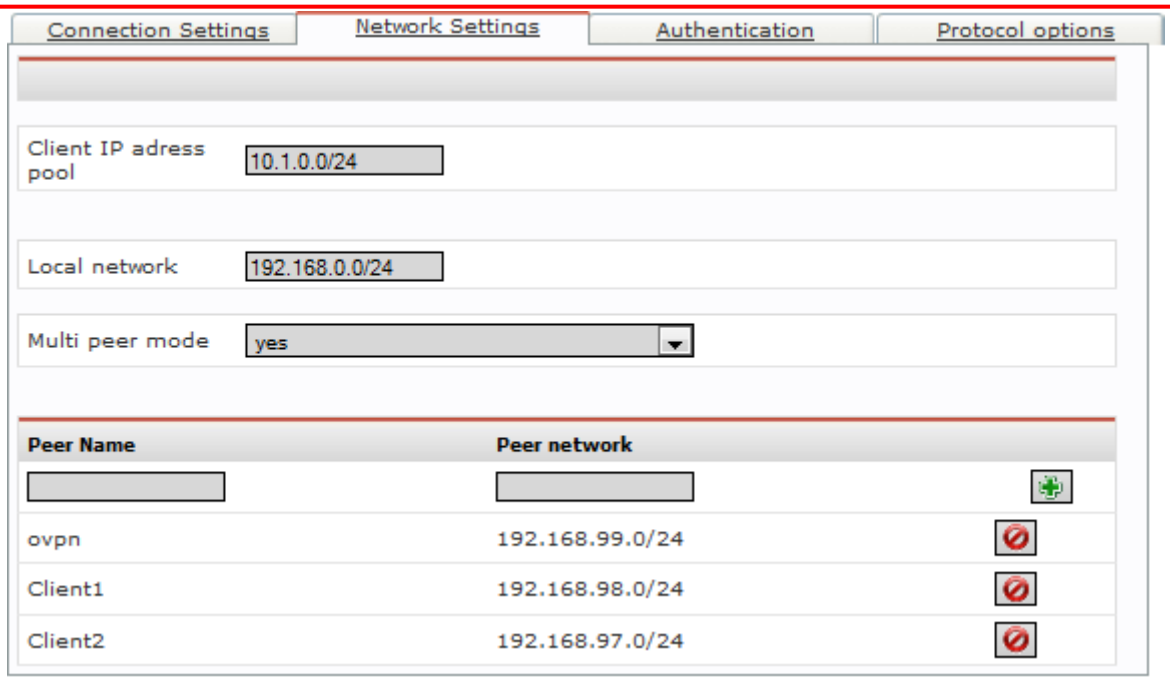


Figure 184

Tab	Label	Description
Network Settings	**Client IP address pool**	With authentication with certificates, multiple different clients can dial into the server simultaneously and are automatically assigned an IP address from the "Client IP address pool". Enter the address range in CIDR notation. E.g. 10.1.0.0/24
	Local network	Enter the address range of the local network in CIDR notation here. E.g. 10.1.0.2/24
	Multiple peers with different network addresses can establish a VPN connection.	"yes" selected With authentication with certificates and this operating mode, multiple clients can dial into the server simultaneously and are automatically assigned an IP address from the "Client IP address pool".
	Peer Name	The local network (top) and the peer network must be specified. Each client is assigned a network in the list below these. Depending on the authentication setting (with certificate name or username), the CN (common name in the certificate) or username will be used. OpenVPN creates an appropriate routing entry for the client currently dialing in.

No network setting is needed on the client because it is sent to the client by the server.

18.2.2.3 **Client authentication: No or static key**

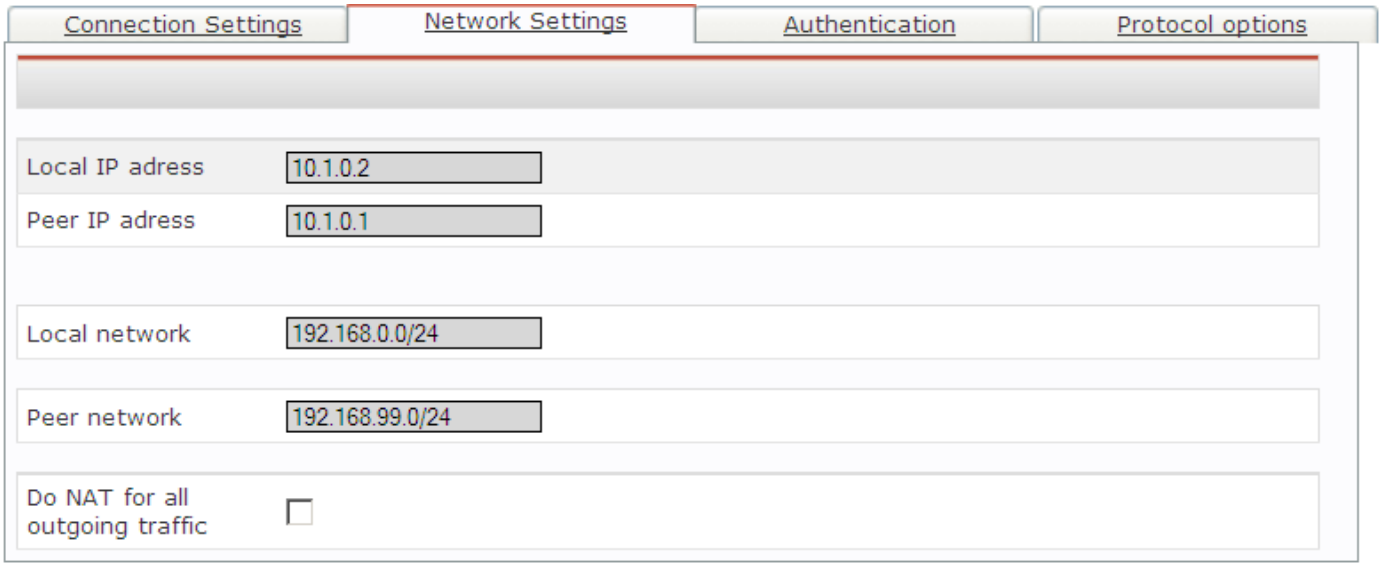


Figure 185

Tab	Label	Description
Network Settings	**Local IP address**	Enter the IP address of the local VPN tunnel end point here, e.g. 10.1.0.2
	Peer IP address	Enter the IP address of the peer VPN tunnel end point here, e.g. 10.1.0.1
	Local network	Enter your network address in CIDR notation here (192.168.0.0/24).
	Peer network	Enter the network address of your peer in CIDR notation here (192.168.99.0/24).
	Do NAT for all outgoing traffic	This option was introduced for compatibility with mdex. It replaces the sender IP address with the current Internet IP address.

With authentication without certificates, only one IP channel can be specified per connection entry (local IP address and peer IP address).

The setting "Local IP address" and "Peer IP address" from the server must be reversed accordingly on the client.

18.2.2.4 **Client authentication: With certificates**

Figure 186

Tab	Label	Description
Network Settings	**Do NAT for all out-going traffic**	This option was introduced for compatibility with mdex. It replaces the sender IP address with the current Internet IP address.

No network setting is needed on the client because it is sent to the client by the server.

18.2.3 Authentication

OpenVPN offers three fundamentally different authentication methods.

- None: no certificate or key is needed. Used primarily for testing the connection. The tunnel data is also NOT encrypted.
- Static key: a key as required by each peer is generated for the connection. Similar to the password.
- Certificates, X.509: the following three certificate variants are distinguished:
  - Each subscriber needs the same root CA and a personal certificate signed by the root CA.
  - Like 1, but with additional username/password verification.
  - Like 2, but without a personal certificate. In other words, subscribers only need a root CA and username/password.

18.2.3.1 No authentication

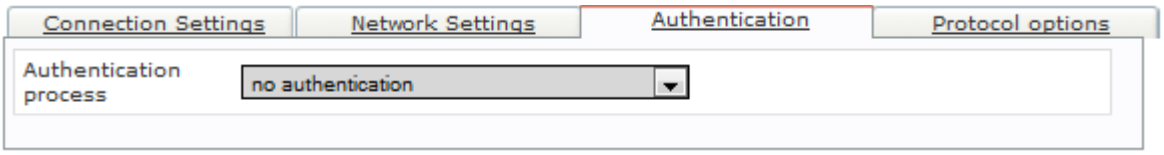


Figure 187

This setting should primarily be used for test purposes. It provides a quick and easy way of testing the connection with a peer (e.g. whether the correct ports are enabled). The data is sent UNENCRYPTED in this mode.

18.2.3.2 Authentication with static key

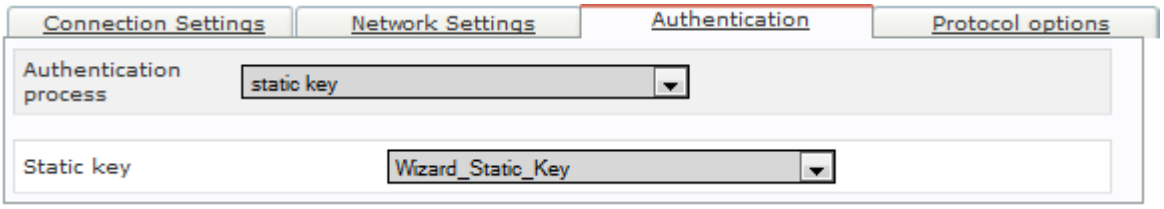


Figure 188

With symmetric encryption, authentication and encryption/decryption of the data is performed using one and the same key (static key). The advantage of symmetric encryption is its speed: encryption and decryption take much less time than with asymmetric encryption since the symmetric key is secure from a size of 90 bits. The asymmetric key, on the other hand, must be at least 1024 bits. The disadvantage of symmetric encryption is that stations need to exchange keys. Each subscriber must obtain the key in a secure manner.
A previously imported or generated key can be selected in the screen shown above.

18.2.3.2.1 Key management

You can import a key or generate it yourself. All imported keys can be downloaded as a copy under "Download".

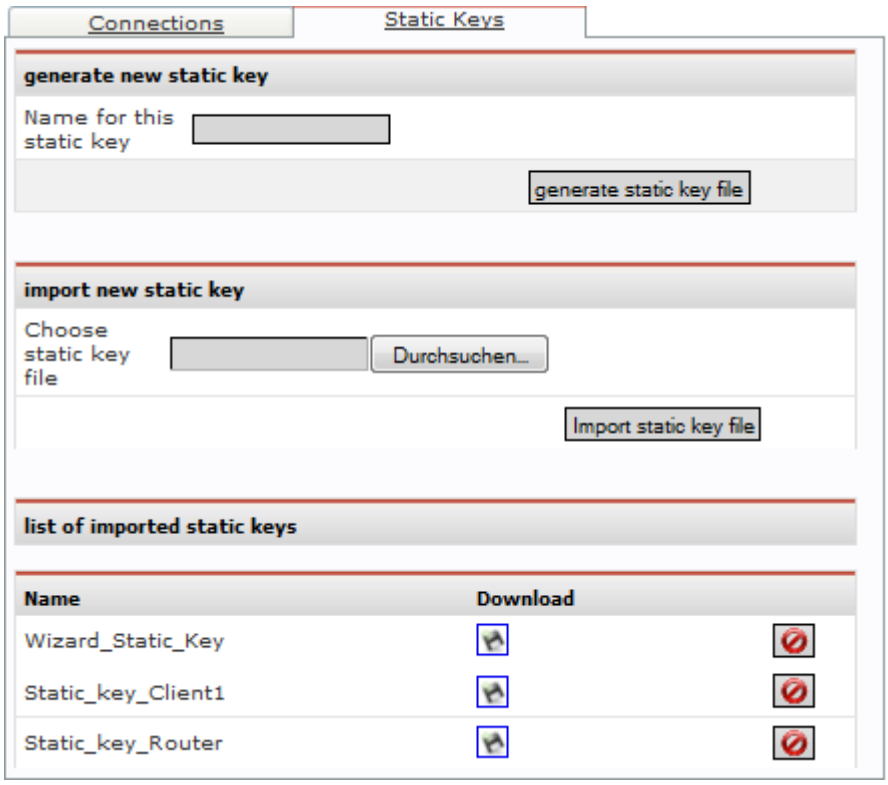


Figure 189

Tab	Label	Description
Static Keys	**Name for this static key**	Enter the name of the key to be generated here.
	Choose static key file	A key previously generated on another system can be imported here.

18.2.3.3 Authentication with certificates

There are three different types of authentication with certificates:

1. Each subscriber needs the same root CA and a personal certificate signed by the root CA.
2. Like 1, but with additional username/password verification.
3. Like 2, but without a personal certificate. In other words, the stations only need a root CA and username/password.

18.2.3.3.1 Authentication with CA certificate and own certificate

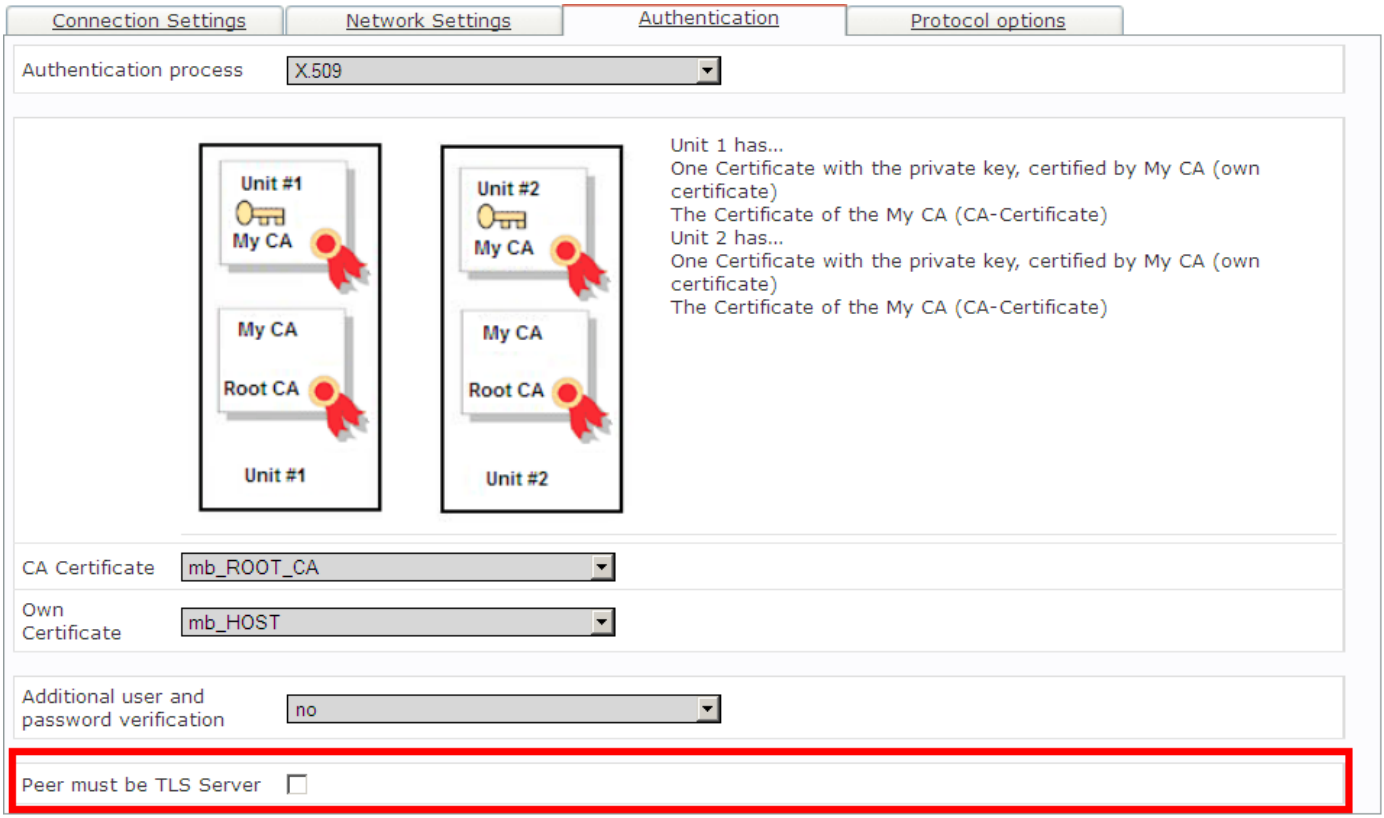


Figure 190

Tab	Label	Description
X.509 authentication	**CA Certificate**	This is the root certificate (root CA). All other certificates must come from this certificate.
	Own Certificate	You use this certificate to authenticate yourself to your VPN peer.
	Additional user and password verification	Additional user data may be required from a client dialing in. Please note that this user data must be entered in the VPN server under *System User*.
	User	Enter the user data of the VPN server (from the System User menu) here.

	Use only CA and User/password for client verification	With this option, you authenticate yourself using the CA certificate and the user data of the VPN server (from the System User menu) only.
	Peer must be TLS Server	This is an additional security option. The "server certificate" must include the extension `nsCertType=server` (see section Creating certificates).

18.2.3.3.2 Authentication with CA certificate and own certificate and user/password

This setting varies depending on the mode.

18.2.3.3.3 Server

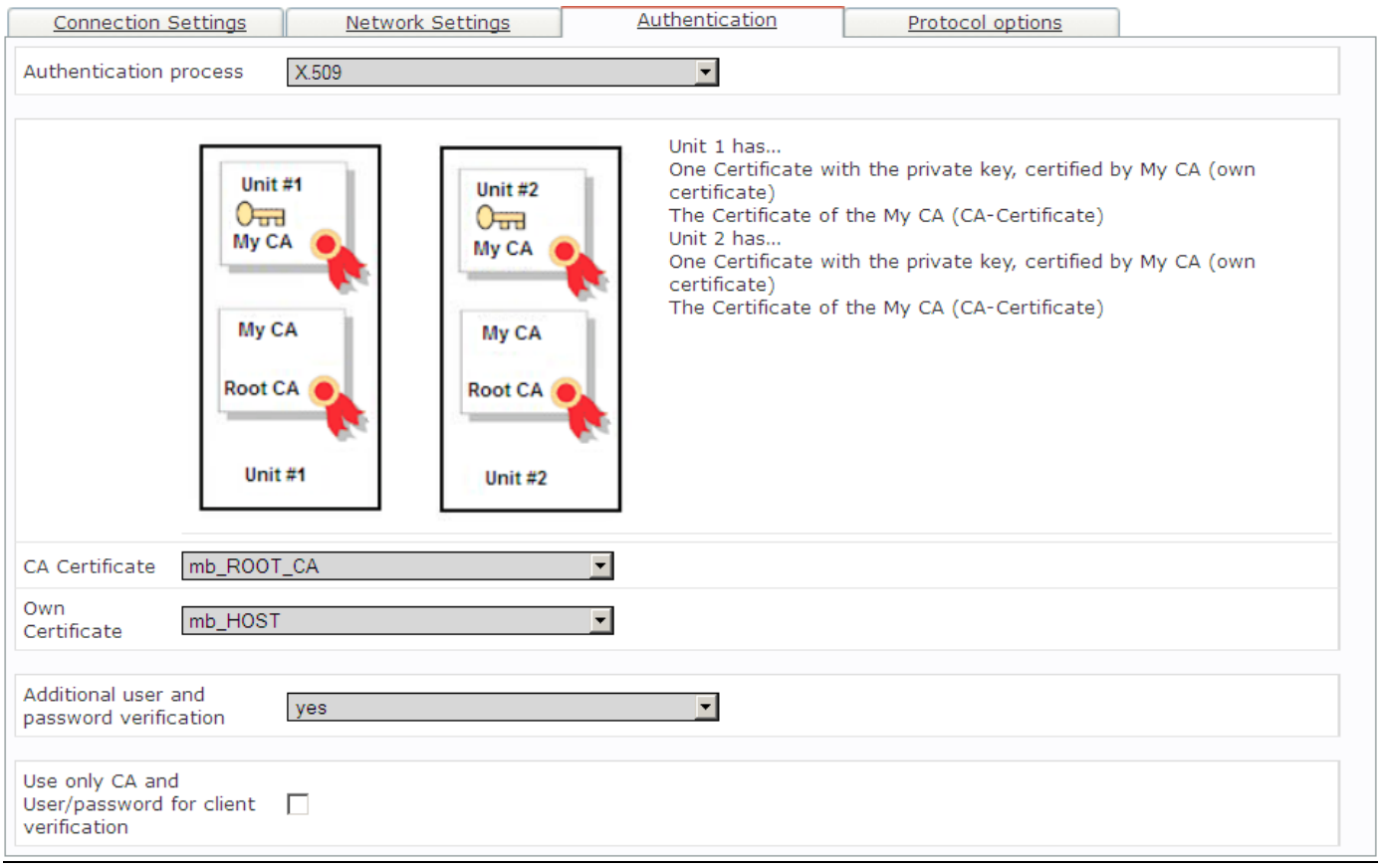


Figure 191

Tab	Label	Description
X.509 authentication (server)	**CA Certificate**	This is the root certificate (root CA). All other certificates must come from this certificate.
	Own Certificate	You use this certificate to authenticate yourself to your VPN peer.
	Additional user and password verification	Additional user data may be required from a client dialing in. Please note that this user data must be entered in the VPN server under *System User*.
	Use only CA and User/password for client verification	With this option, you authenticate yourself using the CA certificate and the user data of the VPN server (from the System User menu) only.

18.2.3.3.4 Client

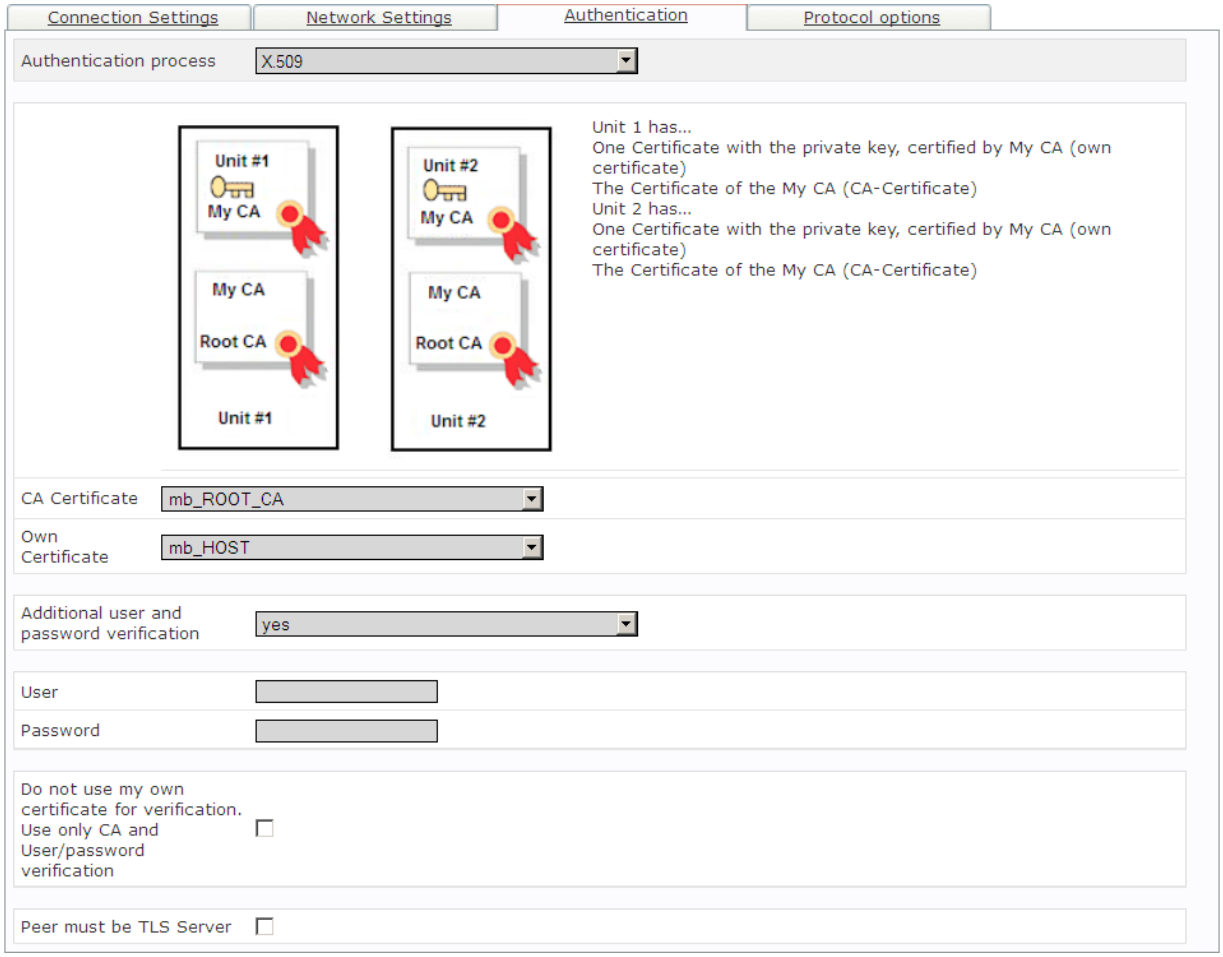


Figure 192

Tab	Label	Description
X.509 authentication (client)	**CA Certificate**	This is the root certificate (root CA). All other certificates must come from this certificate.
	Own Certificate	You use this certificate to authenticate yourself to your VPN peer.
	Additional user and password verification	Additional user data may be required from a client dialing in. Please note that this user data must be entered in the VPN server under *System User*.
	User	Enter the user data of the VPN server (from the System User menu) here.
	Do not use my own certificate for verification. Use only CA and User/password for verification	With this option, you authenticate yourself using the CA certificate and the user data of the VPN server (from the System User menu) only.
	Peer must be TLS Server	This is an additional security option. The "server certificate" must include the extension `nsCertType=server` (see section Creating certificates).

18.3 Inactivity settings

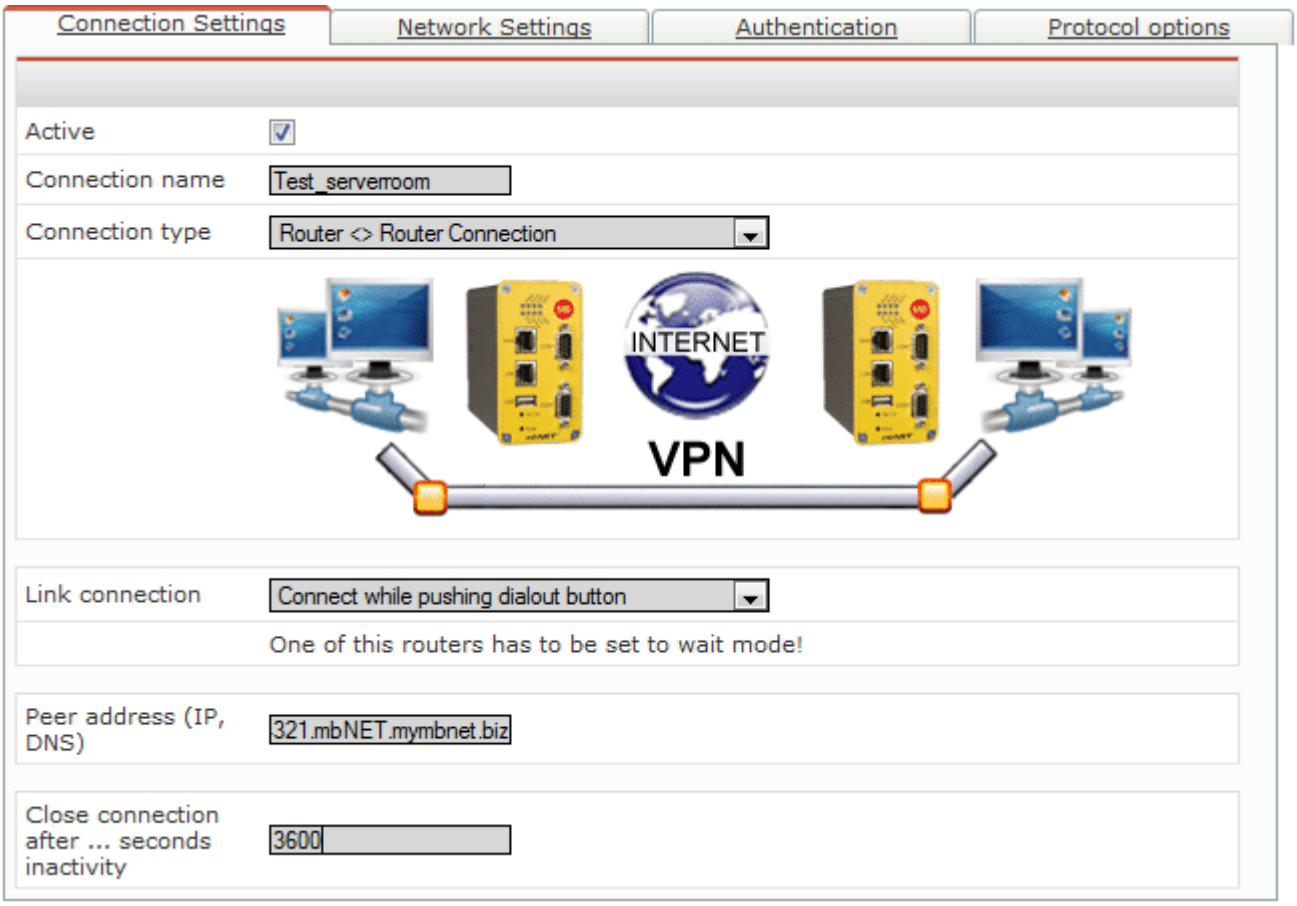


Figure 193

18.4 Protocol options

If the OpenVPN connection is to be started via a digital input or the dial-out button, the connection is automatically dropped after a defined time without any data traffic. on

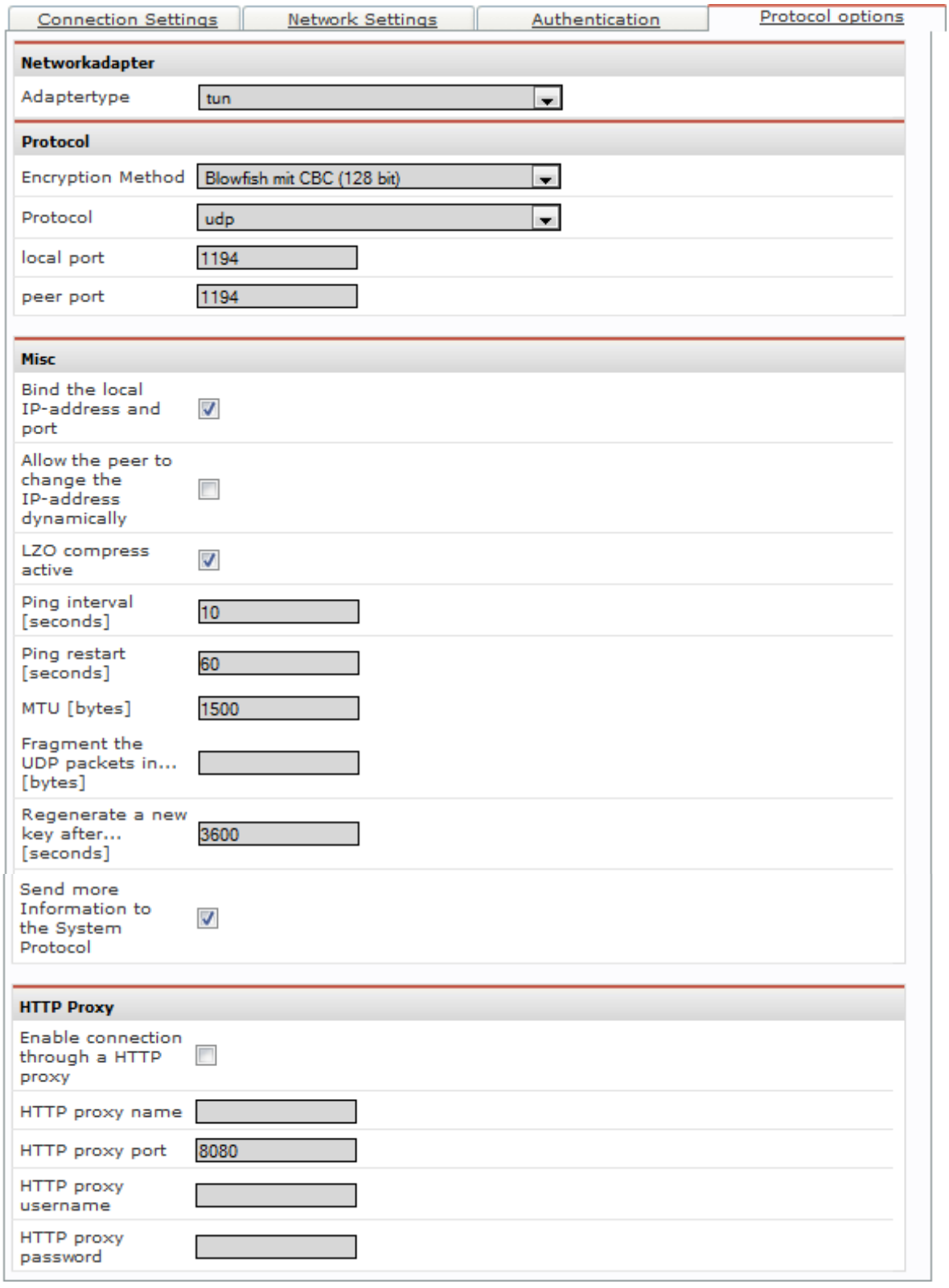
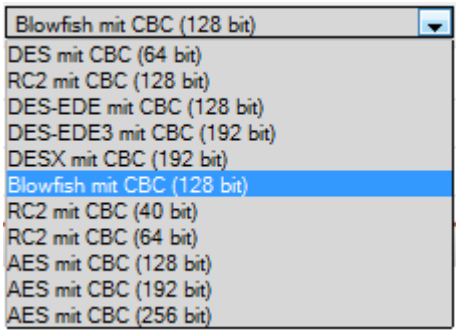


Figure 194

Tab	Label	Description
Protocol options	**Encryption Method**	 **Figure 195** This setting must be the same on the peers.
	Protocol	UDP or TCP can be selected. The default setting is UDP. If the http proxy is selected, TCP is automatically valid.
	local/peer port	OpenVPN communication is conducted via the set ports. These ports generally have the same settings. The default port is 1194.
	Bind the local IP-address and port.	OpenVPN cannot change the ports dynamically while the connection is active.
	Allow the peer to change the IP-address dynamically	This option allows the VPN peer to change its IP address while the connection is active.
	LZO compress active	Compression method of OpenVPN.
	Ping interval [seconds]	A ping is sent to the VPN peer if the OpenVPN tunnel has not been used for n seconds.
	Ping restart [seconds]	The tunnel is restarted if the VPN peer does not respond to the ping within n seconds or no data packet is received.
	MTU [bytes]	The default MTU size is 1500 bytes.
	Fragment the UDP packets in ... [bytes]	Packets bigger than n bytes will be fragmented.
	Regenerate a new key after ... [seconds]	A new key will be generated after n seconds. This is set to 3600 seconds by default.

	Send more Information to the System Protocol	This corresponds to the "verb 3" setting of OpenVPN. The default is "off".
	Enable connection through a HTTP proxy	You must check this box if you want to establish your connection with the Internet via an http proxy server.
	HTTP proxy name	Enter the IP address or DNS name of the proxy server here.
	HTTP proxy port	Enter the port via which your proxy server accepts requests here (e.g. 8080 or 3128).
	HTTP proxy username	If your proxy server requests authentication, enter a valid username and the associated password.

19. I/O Manager

The I/O Manager integrated in the router performs the following functions:

- Displays PLC variables
- Reads variables from the PLC and saves them to the USB stick at a set interval (logging).
- Places the logged archives (GZIP) on an external FTP server at a fixed interval.

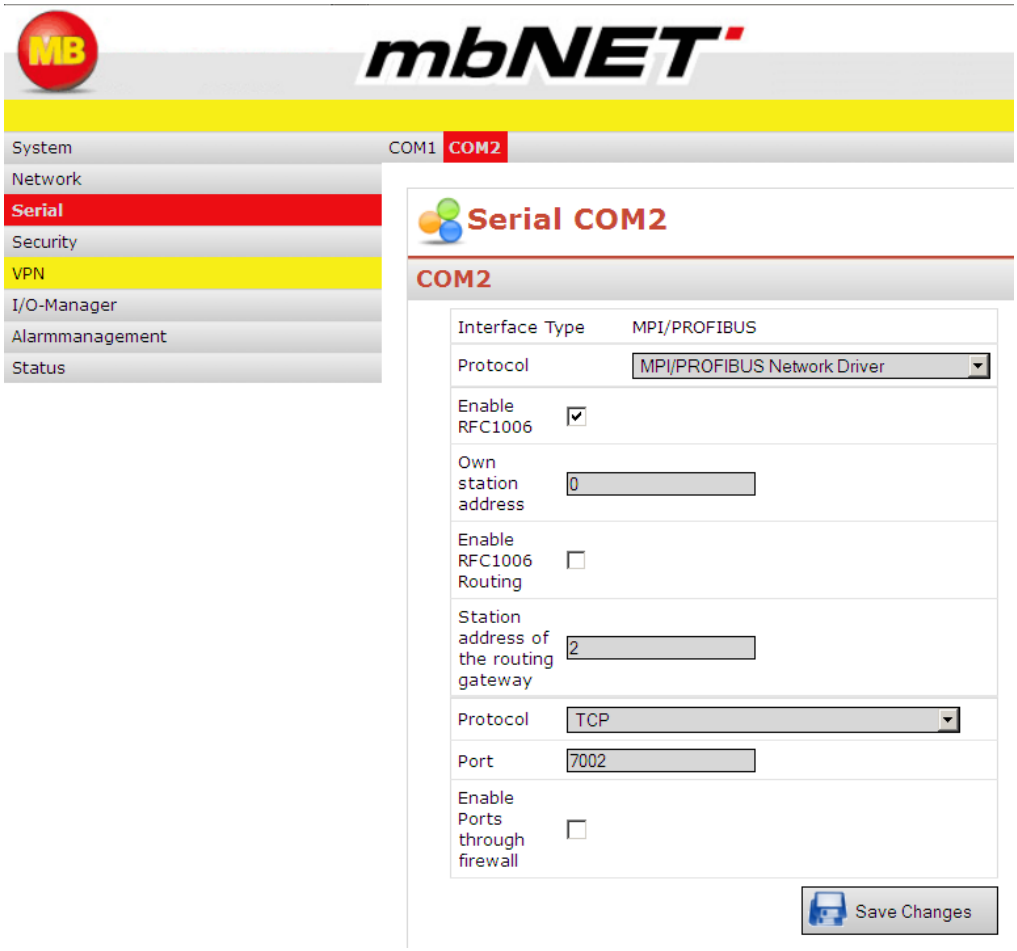
Variables of the type flags, times, counters, inputs, outputs, data blocks and peripherals can currently be read from an S7 controller via RFC1006. The PLC can communicate directly with the router via its Ethernet interface or via the MPI/PROFIBUS interface of the router.

Limits:

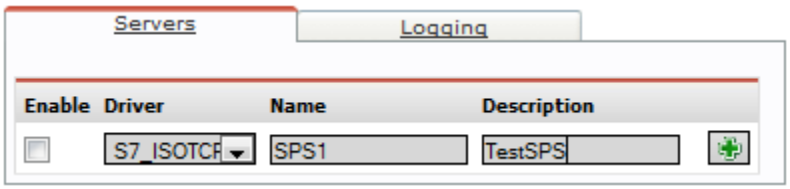
- Max. 4 connections to the controllers
- Max. 256 tags (variables) per connection
- The maximum size of a tag is one DWORD (32 bits)

19.1 Configuring the connection

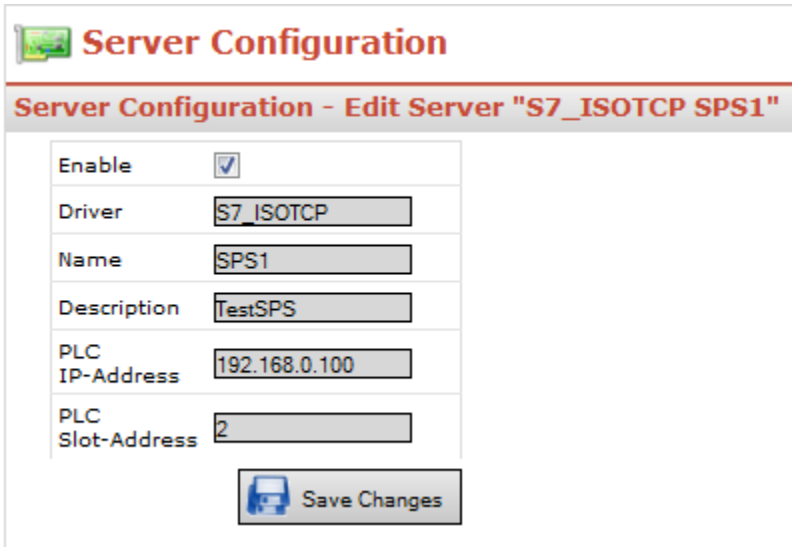
If using the MPI/PROFIBUS interface of the router, the RFC1006 protocol must first be activated for this interface.



19.1.1 Creating the PLC connection



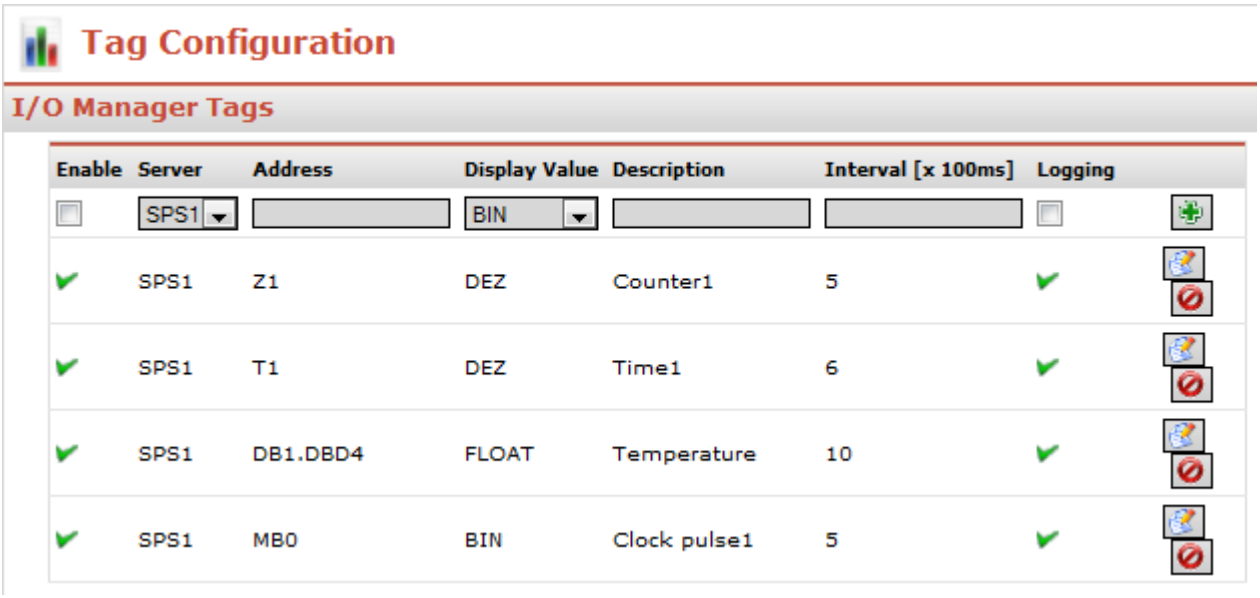
The "Name" field must not contain any control characters or spaces. Click the "+" button after entering the data.



If using the MPI/PROFIBUS interface, the IP of the router's LAN interface must be entered in the PLC IP-Address field. Otherwise the IP address of the PLC. The slot address is the bus address with MPI/PROFIBUS communication and, in the case of direct Ethernet communication, the slot space of the PLC on the rack (generally two).

19.1.2 Creating the tags

Tags can be added if there is at least one PLC connection created.


Tag Configuration
I/O Manager Tags
Enable Server Address Display Value Description Interval [x 100ms] Logging
SPS1 BIN
SPS1 Z1 DEZ Counter1 5
SPS1 T1 DEZ Time1 6
SPS1 DB1.DBD4 FLOAT Temperature 10
SPS1 MB0 BIN Clock pulse1 5

The following address syntax must be used for this driver:

DBx.DBXy.z = data block x, data bit y.z, BOOL

DBx.DBBy = data block x, data byte y, BYTE

DBx.DBWy = data block x, data word y, WORD

DBx.DBDy = data block x, data double word y, DWORD

Fy.z = flag bit y.z, BOOL

FBy = flag byte y, BYTE

FWy = flag word y, WORD

FDy = flag double word y, DWORD

Iy.z = input bit y.z, BOOL

IBy = input byte y, BYTE

IWy = input word y, WORD

IDy = input double word y, DWORD

Oy.z = output bit y.z, BOOL

OBy = output byte y, BYTE

OWy = output word y, WORD

ODy = output double word y, DWORD

PIy.z = peripheral input bit y.z, BOOL

PIBy = peripheral input byte y, BYTE

PIWy = peripheral input word y, WORD

PIDy = peripheral input double word y, DWORD

Ty = Timer y, TIMER

Cy = Counter y, COUNTER

Display format This format is used for the status display and in the logging data.

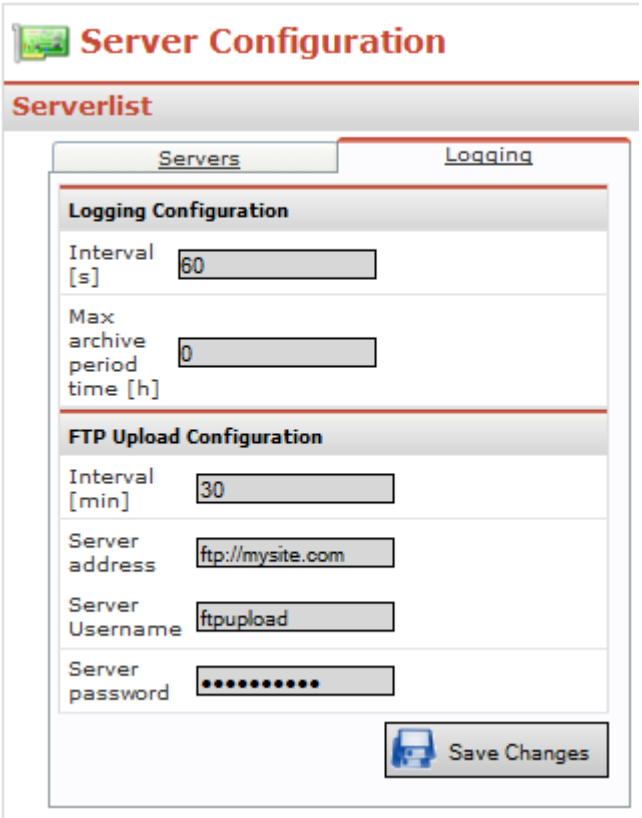
Description Free label field.

Interval [x 100ms] This tag is read from the PLC during this interval.

Logging This tag is enabled for logging if this option is checked. The tag is only displayed on the status display if this option is not checked.

19.2 Configuring the logging function

The logging function can be configured on the second tab under Server Configuration. The logging function applies to all PLC connections.



A storage medium must be inserted into the USB socket for the logging function. This can be e.g. a USB stick.

Interval [s] The tags are written to the storage medium at the specified interval.

Max archive period time [h] The log file is archived and a new log file is started at the latest after

the time in seconds set here.

FTP Upload Configuration

The logged tags can also be archived on an FTP server. The following settings are required for this.

The "Maximum" firewall security setting does not permit the agreement of a dynamic communication port as required during FTP communication between the client and server. The router firewall must therefore be set to "Normal" in this case.

Interval [min] The log file is compressed and loaded onto the FTP server at the specified interval. A copy of the log file also remains on the storage medium (compressed).

Server address Enter the address of the FTP server here.

Server Username Enter the username for authentication on the FTP server here.

Server password Enter the password for authentication on the FTP server here.

Log files are in CSV format. The current file is always called logfile.log and is stored in the subdirectory \logfiles\ on the USB stick. Archived files use the following naming convention: logfile.log.[Date(yyyymmdd)]_[Time(hhmmssms3)].gzip

20. Alarm management

20.1 General

The alarm management function can be used to

- query the states at the four digital inputs and, depending on the result, send an appropriate text to an email address you have specified.
- switch two digital outputs independent of each other in the event of a fault, when there is an active Internet connection or manually.

20.2 Digital inputs

Click **Alarmmanagement** in the navigation bar, followed by **Input**.

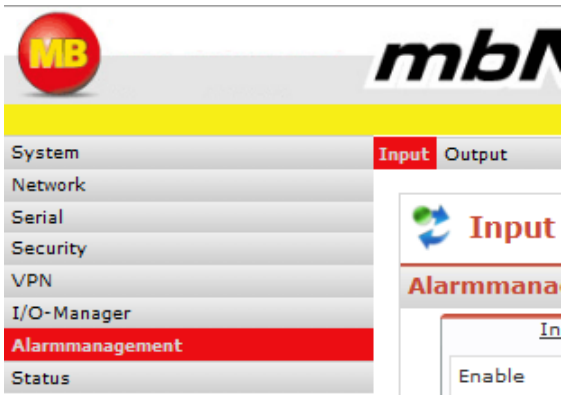


Figure 196

The following screen for configuring the four available digital inputs is then displayed. The inputs can be individually configured using the four different tabs.

Alarmmanagement (continued)

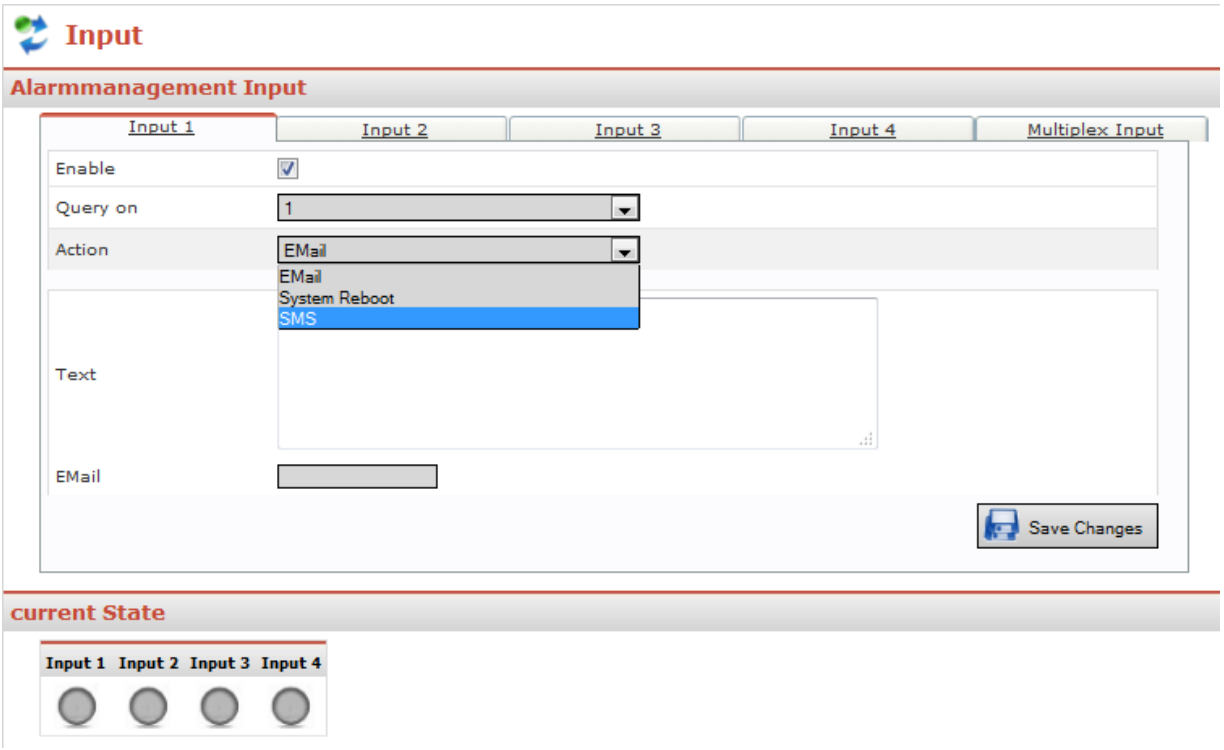


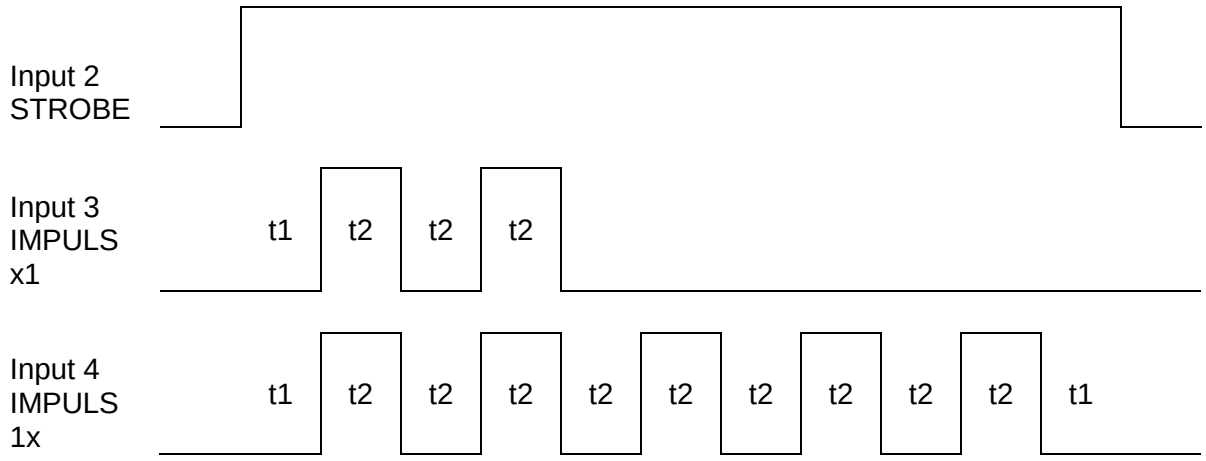
Figure 197

Label	Function
Input 1 .... 4 tabs	Each input can be separately configured. Select the input to be configured by clicking the corresponding tab.
Enable	The input is enabled by checking the box. This is how you determine whether the input in question is to be enabled ("activated").
Query on	Set the input level for the industrial router in this drop-down field. The available signal levels are 1 and 0.
Action	There are three possible actions: ☐ EMail ☐ SMS ☐ System Reboot
Text	Enter the text to be sent to the specified email address in this input field. The following special characters are permitted in the text: ÄÜÖ,;.:-_#+*~^°!()=?§$%&/<>
EMail/Mobile Phone	Enter the email address or phone number to which the industrial router should send the text when the input is activated and the relevant signal level has resulted in the action being initiated.
current State	You can read off the current state at the inputs via the LED icons at the bottom of the screen. Gray indicates state 0, green indicates state 1.

20.2.1 **Multiplex inputs**

Brief description:
There are four digital inputs on the mbNET. An action assignment (number) can be communicated serially via three of these inputs (2-4), i.e. one input is STROBE, one is IMPULS_x1 and one is IMPULS_1x. The pulse at IMPULS_x1 (one digit) and IMPULS_1x (tens digit) can be counted with a rising edge at STROBE. The action is executed in accordance with the entered action with a falling edge at STROBE.

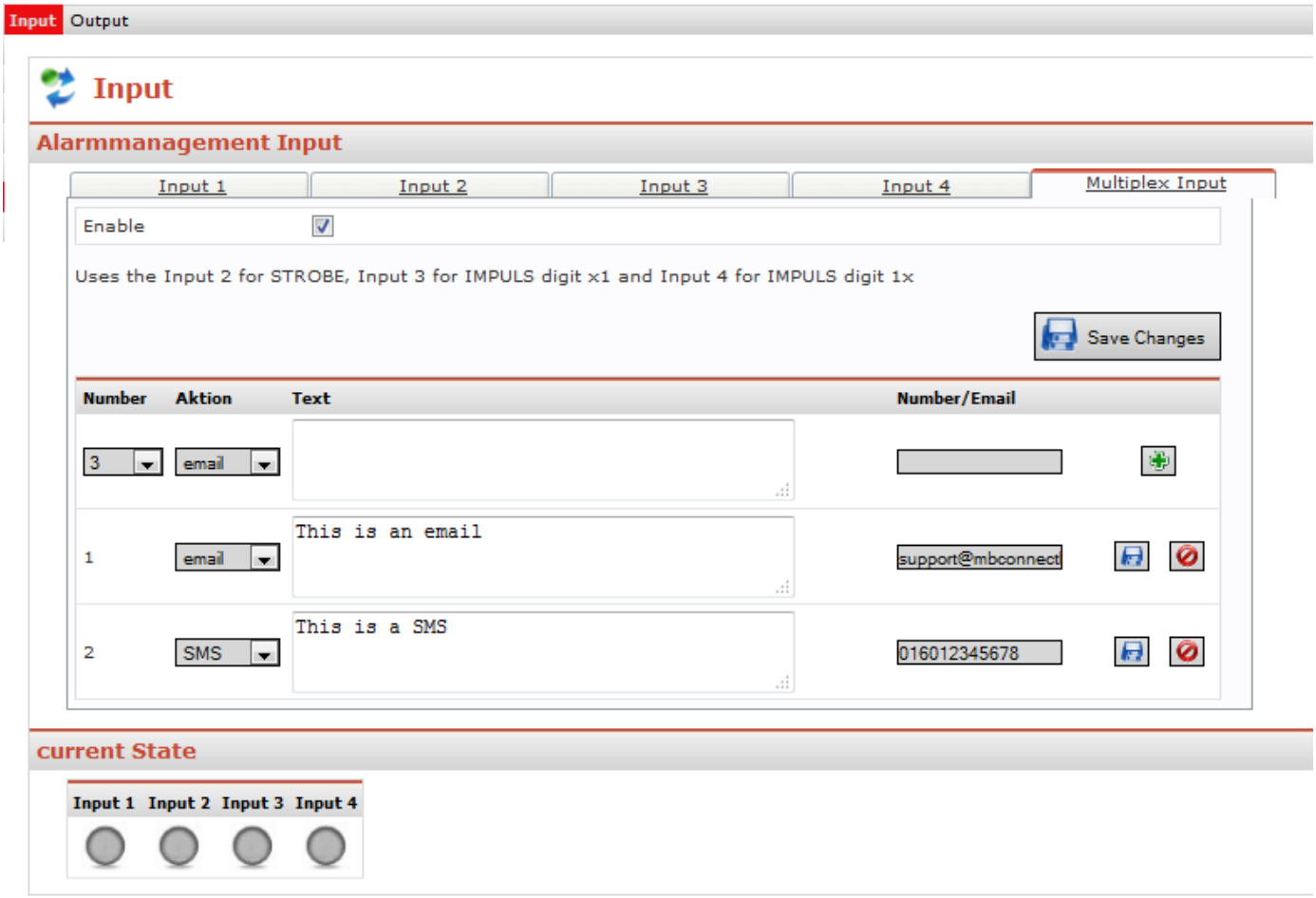
Graph



t1 > 50 ms
t2 > 100 ms

The action **52** is initiated in the sample graph.

Action table



The action number is defined in the Number drop-down field. There are different actions available depending on device model. The "EMail" function is available with all devices, the "SMS" option is available with devices with a mobile broadband modem.

20.3 Digital outputs

Click **Alarmmanagement** in the navigation bar, followed by **Output**.

The following screen for configuring the two available digital outputs is then displayed. The outputs can be separately configured using the two tabs.
The input and drop-down fields are described on the following pages.

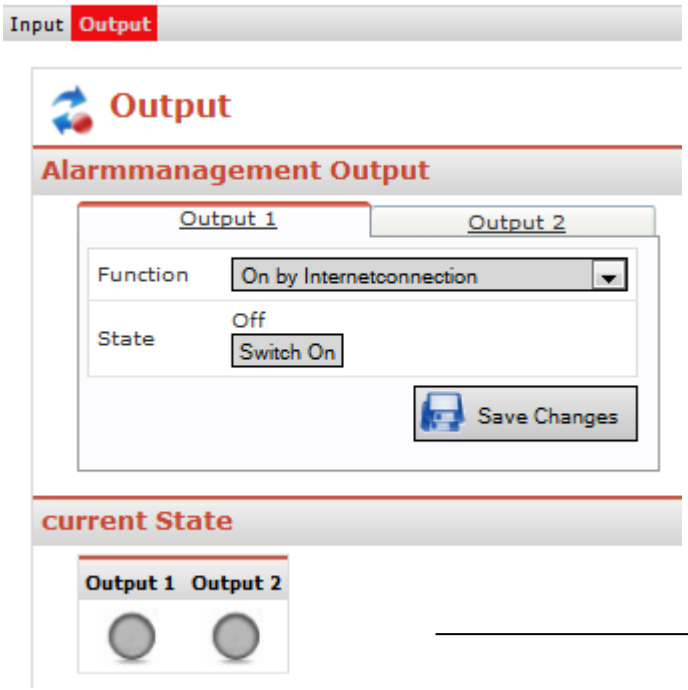


Figure 198

Label	Function
Output 1 Output 2	Each output can be separately configured. To configure an output, select the corresponding tab.
Function	You can chose between the following settings using the drop-down field: **Off** Select this setting if you do not want to evaluate the outputs for possible switching operations. **On with Malfunction** Select this setting if the corresponding output of the industrial router is to be set to signal level 1 in the event of a malfunction. **On by Internetconnection** Select this setting if the corresponding output of the industrial router is to be set to 1 in the event of an active Internet connection. For example, an active Internet connection can then be indicated by an LED connected at output O1 or O2.

State	**Switch On** or **Switch Off** This button can be used to switch the currently selected output on and off. The text **Off** or **On** above the button shows the current output state in the same way as the LED icons under **current State**. **Green LED icon:** Signal level 1 at output **Gray LED icon:** Signal level 0 at output

21. Status messages

21.1 General

The industrial router must be analyzed using certain status information when errors occur. For example, a flashing ERROR LED indicates that a system error has occurred on the router. The cause of the error can be determined e.g. via **Status** – **System** using the list.
The various status displays are described below:

21.2 Status – Interfaces

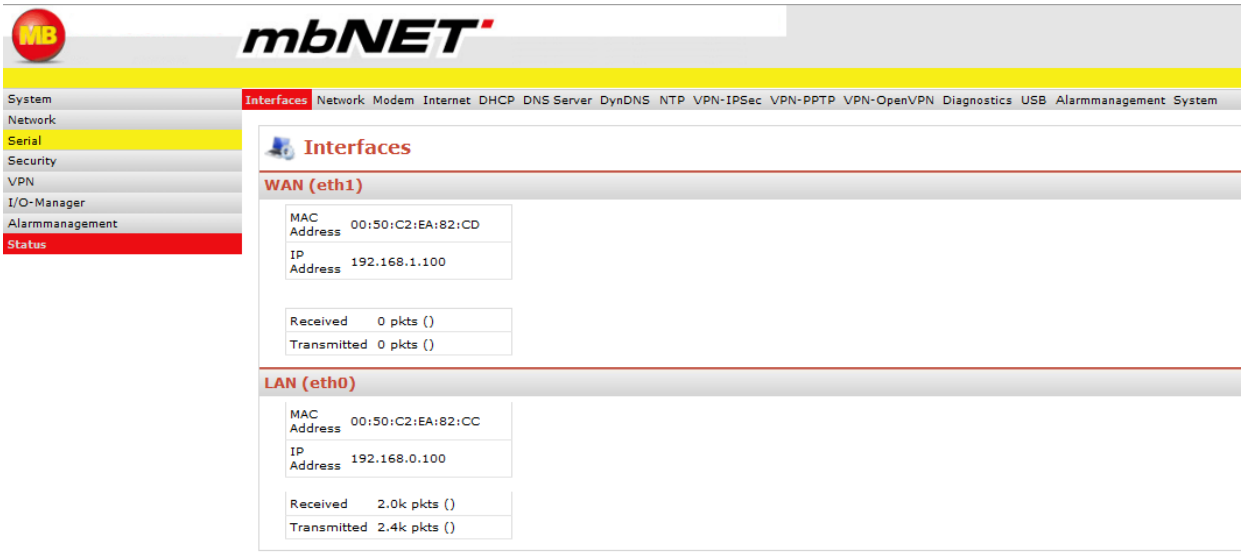


Figure 199

Label	Function
WAN	Shows the settings at the router's WAN connection (external connection). The IP address is displayed as soon as the router has a physical connection to the network or is assigned a static IP address. The number of data packets received and transmitted is displayed.
LAN	Shows the settings at the router's LAN connection (local connection). The IP address is displayed when the router has a physical connection. The number of data packets received and transmitted is displayed.

21.3 Status – Network

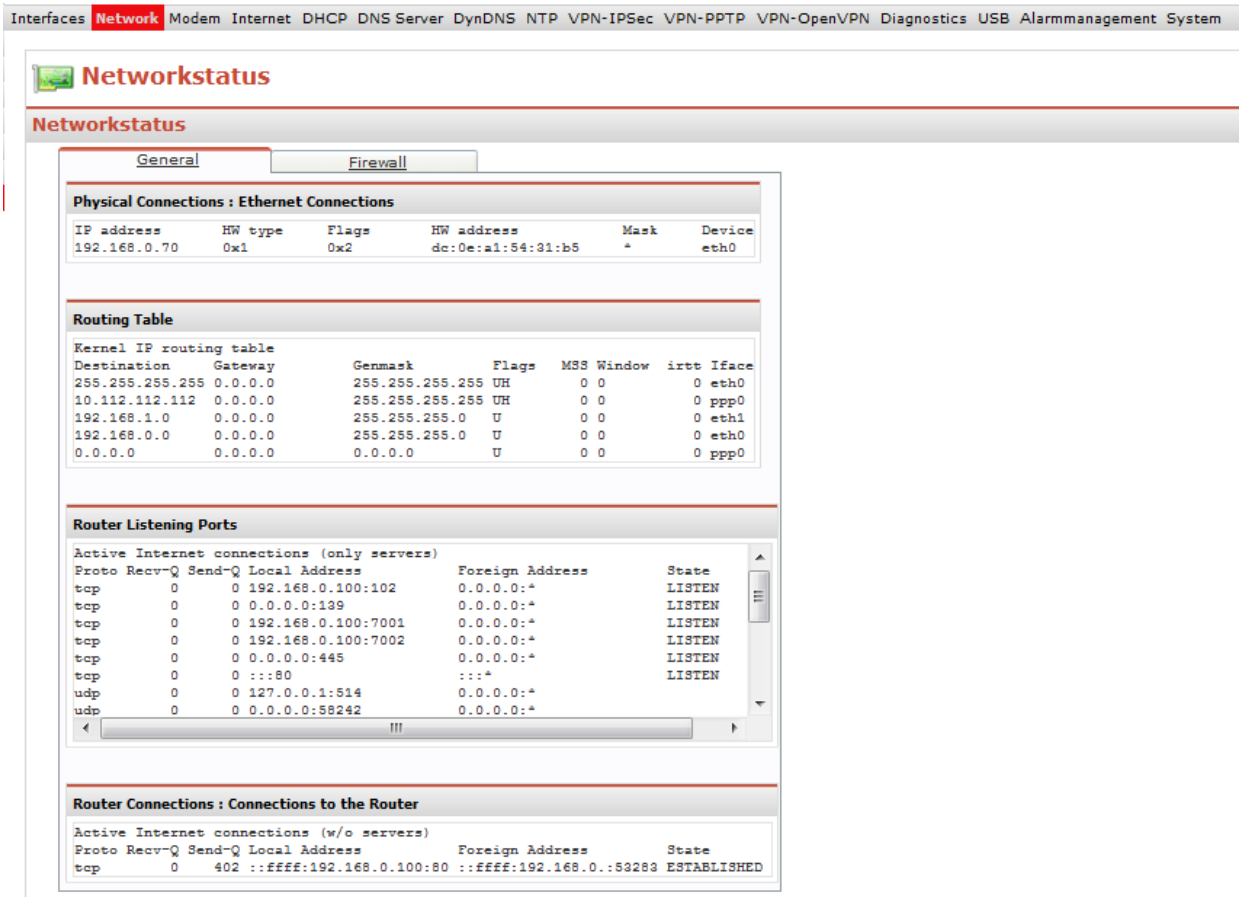

Interfaces Network Modem Internet DHCP DNS Server DynDNS NTP VPN-IPSec VPN-PPTP VPN-OpenVPN Diagnostics USB Alarmmanagement System
Networkstatus
Networkstatus
General
Firewall
Physical Connections : Ethernet Connections
IP address HW type Flags HW address Mask Device
192.168.0.70 0x1 0x2 dc:0e:a1:54:31:b5 * eth0
Routing Table
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
255.255.255.255 0.0.0.0 255.255.255.255 UH 0 0 0 eth0
10.112.112.112 0.0.0.0 255.255.255.255 UH 0 0 0 ppp0
192.168.1.0 0.0.0.0 255.255.255.0 U 0 0 0 eth1
192.168.0.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
0.0.0.0 0.0.0.0 0.0.0.0 U 0 0 0 ppp0
Router Listening Ports
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 192.168.0.100:102 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:139 0.0.0.0:* LISTEN
tcp 0 0 192.168.0.100:7001 0.0.0.0:* LISTEN
tcp 0 0 192.168.0.100:7002 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:445 0.0.0.0:* LISTEN
tcp 0 0 :::80 :::* LISTEN
udp 0 0 127.0.0.1:514 0.0.0.0:*
udp 0 0 0.0.0.0:58242 0.0.0.0:*
Router Connections : Connections to the Router
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 402 ::ffff:192.168.0.100:80 ::ffff:192.168.0.:53283 ESTABLISHED

Figure 200

Label	Function
Physical Connections	Shows the physical connections via which the router is connected to other computers.
Routing Table	Shows all routes used.
Router Listening Ports	Shows all monitored ports.
Router Connections: Connections to the Router	Shows all IP addresses with ports, e.g. of computers that are connected to the router.

21.4 Status – Modem

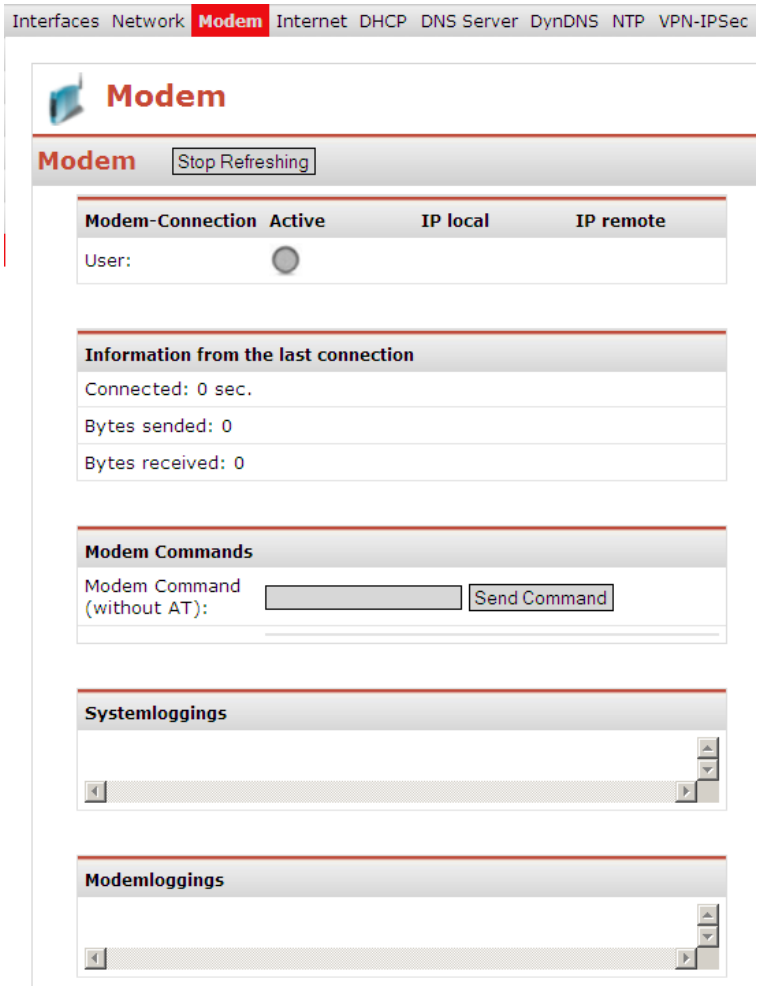


Figure 201

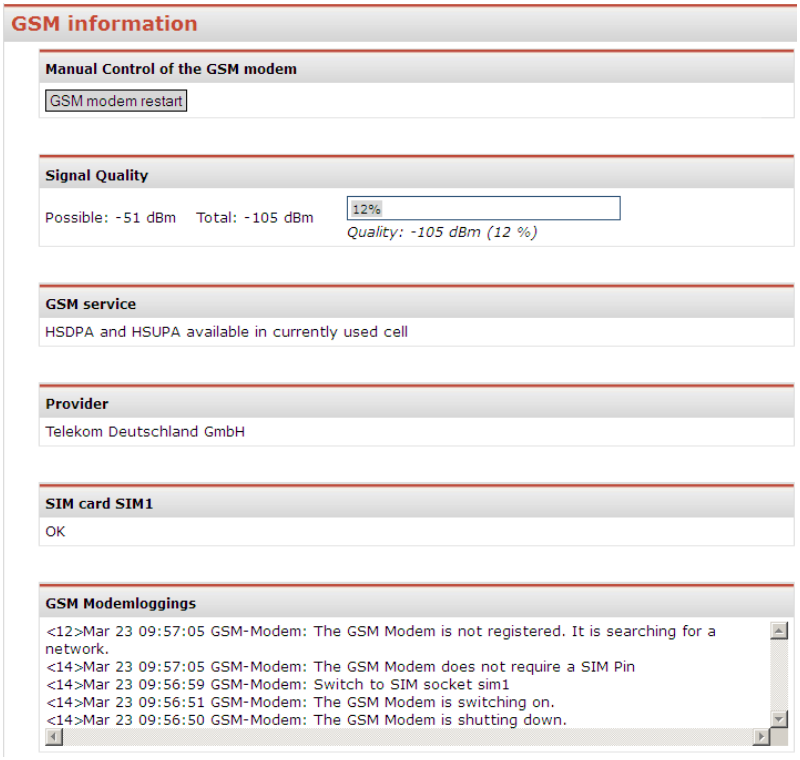

GSM information
Manual Control of the GSM modem
GSM modem restart
Signal Quality
Possible: -51 dBm Total: -105 dBm
12%
Quality: -105 dBm (12 %)
GSM service
HSDPA and HSUPA available in currently used cell
Provider
Telekom Deutschland GmbH
SIM card SIM1
OK
GSM Modemloggings
<12>Mar 23 09:57:05 GSM-Modem: The GSM Modem is not registered. It is searching for a network.
<14>Mar 23 09:57:05 GSM-Modem: The GSM Modem does not require a SIM Pin
<14>Mar 23 09:56:59 GSM-Modem: Switch to SIM socket sim1
<14>Mar 23 09:56:51 GSM-Modem: The GSM Modem is switching on.
<14>Mar 23 09:56:50 GSM-Modem: The GSM Modem is shutting down.

Figure 202

Label	Function
Modem-Connection	Shows the user who dialed into the router via modem. The IP address of the PPP server and PPP client (remote station) is displayed when a dial-up connection is successfully established. The connections are always incoming connections. An active connection is indicated by a green dot.
Information from the last connection	Shows the connection time and the number of bytes sent and received during the most recent connection as long as the router was not restarted or switched off in the interim.
Modem Commands	This input field can be used to issue a command directly to the internal modem.**This function should only be used as directed by MB Connect Line support personnel.**
Systemloggings	Shows the type of connection and the assigned IP and DNS addresses.
Modemloggings	Shows the commands sent to the modem to initialize it and the status of the connection process. The error messages that occur when establishing the connection are also displayed here.
Manual Control of the GSM modem	You can use this button to restart the internal modem. **This function should only be used as instructed by MB Connect Line support personnel.**
Signal Quality	Specifies the current network availability in percent and dBm. If you have an mbNET with mobile broadband and UMTS, the device will automatically change networks when UMTS becomes available again or UMTS is no longer available.
GSM service	Shows the respective transmission method. The following are possible: ☐ GSM/GPRS ☐ EDGE ☐ UMTS
Provider	Shows the current mobile broadband provider (T Mobile Germany as shown in Figure 211).
SIM card SIM1	Shows the status of your SIM card in mbNET.
GSM Modemloggings	Shows all events and errors related to the GSM modem.

21.5 Status – Internet

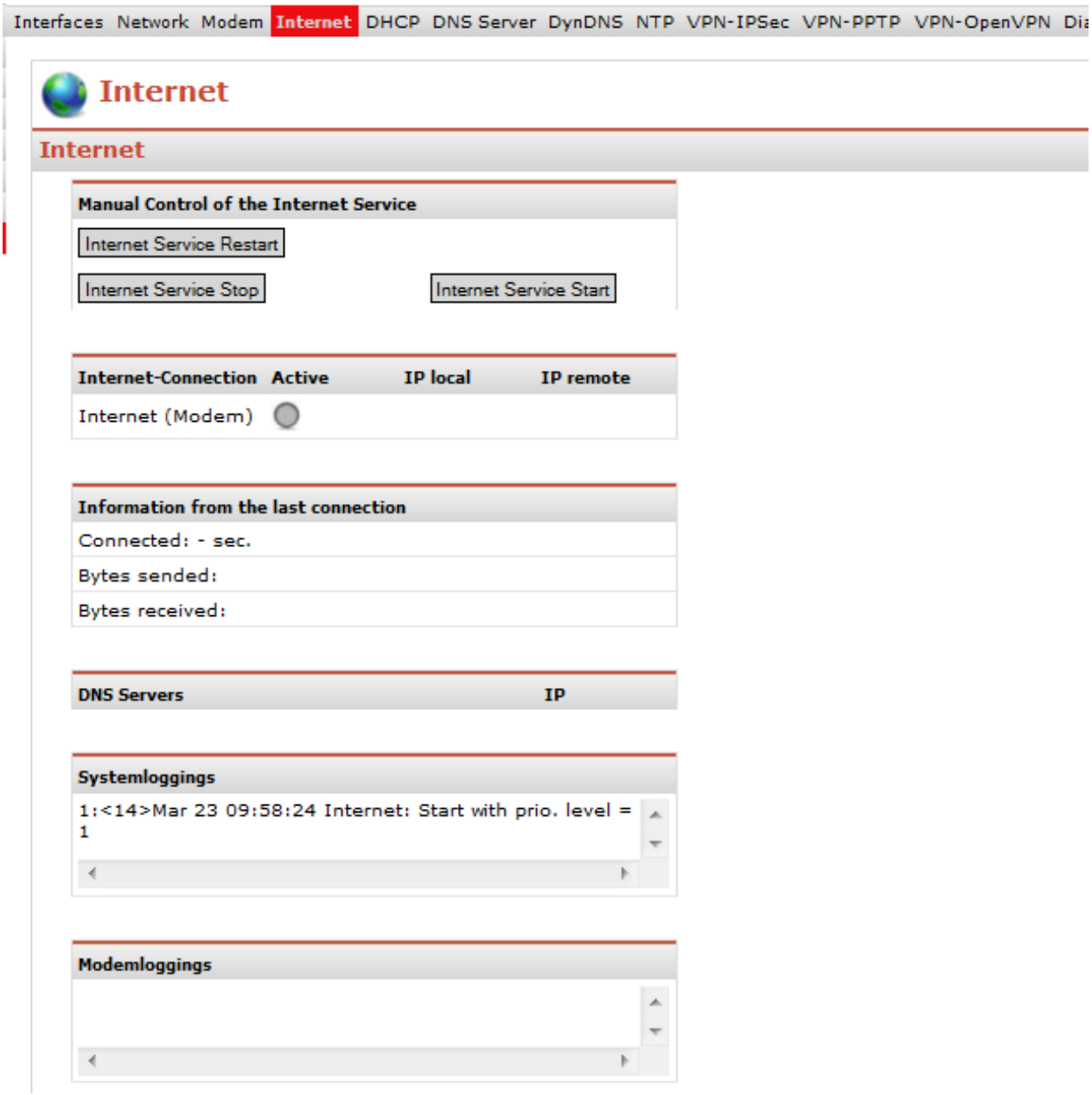
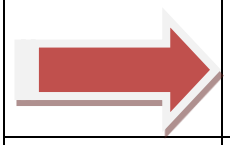


Figure 203

Label	Function
Internet 	Shows outgoing connections to the Internet. These can be both outgoing connections via the modem and connections via WAN. The IP addresses of the local and remote stations are displayed. An active connection is indicated by a green dot. You can manually connect or disconnect the Internet connection here also. **However it is not recommended to use these buttons unless requested to do so by a member of the support team.**
Information from the last connection	Shows the connection time and the number of bytes sent and received during the most recent connection as long as the router was not restarted or switched off in the interim.
DNS Servers	Shows the IP address of the DNS server.
Systemloggings	Shows the type of connection and the assigned IP and DNS addresses.
Modemloggings	Shows the commands sent to the modem to initialize it and the status of the connection process. The error messages that occur when establishing the connection are also displayed here.

21.6 Status – DHCP

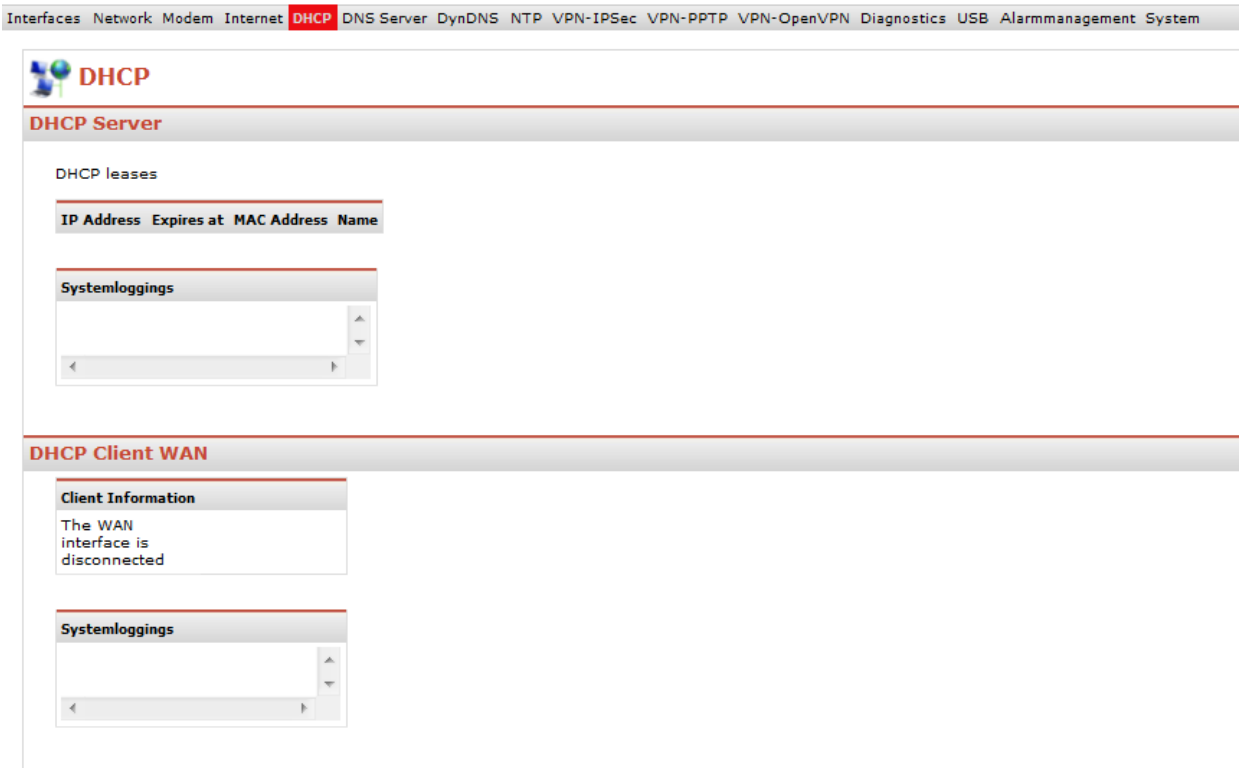

Interfaces Network Modem Internet DHCP DNS Server DynDNS NTP VPN-IPSec VPN-PPTP VPN-OpenVPN Diagnostics USB Alarmmanagement System
DHCP
DHCP Server
DHCP leases
IP Address Expires at MAC Address Name
Systemloggings
DHCP Client WAN
Client Information
The WAN interface is disconnected
Systemloggings

Figure 204

Label	Function
DHCP Server	Lists the IP addresses assigned to connected clients by the DHCP server.
Systemloggings	Shows the IP addresses assigned by the DHCP and the IP addresses that are not permitted.
Client Information	Shows information about connected clients at the WAN connection.
Systemloggings	Shows all events and errors related to the DHCP server and client.

21.7 Status – DNS Server

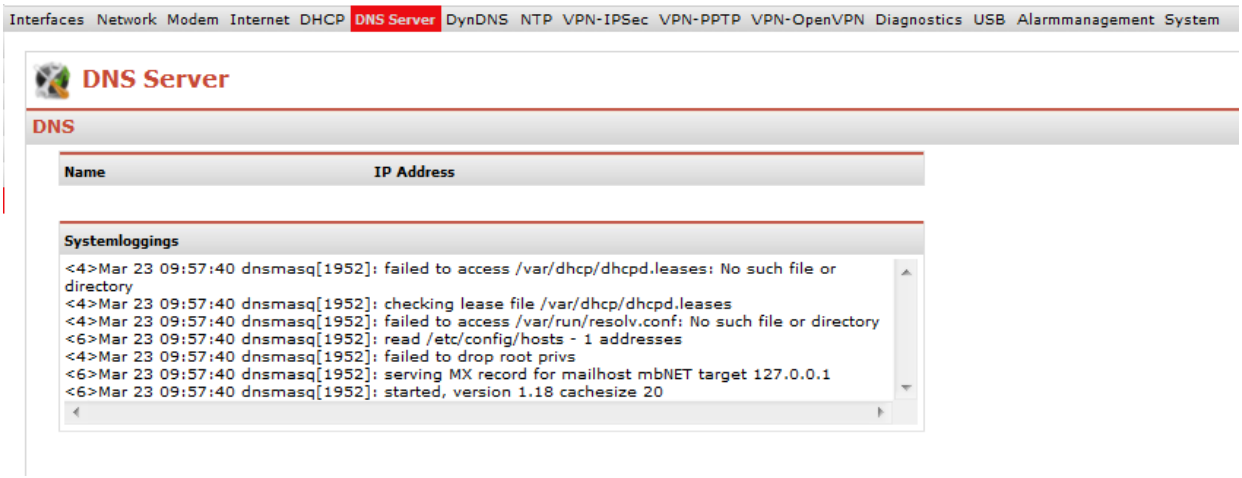

Interfaces Network Modem Internet DHCP DNS Server DynDNS NTP VPN-IPSec VPN-PPTP VPN-OpenVPN Diagnostics USB Alarmmanagement System
DNS Server
DNS
Name
IP Address
Systemloggings
<4>Mar 23 09:57:40 dnsmasq[1952]: failed to access /var/dhcp/dhcpd.leases: No such file or directory
<4>Mar 23 09:57:40 dnsmasq[1952]: checking lease file /var/dhcp/dhcpd.leases
<4>Mar 23 09:57:40 dnsmasq[1952]: failed to access /var/run/resolv.conf: No such file or directory
<6>Mar 23 09:57:40 dnsmasq[1952]: read /etc/config/hosts - 1 addresses
<4>Mar 23 09:57:40 dnsmasq[1952]: failed to drop root privs
<6>Mar 23 09:57:40 dnsmasq[1952]: serving MX record for mailhost mbNET target 127.0.0.1
<6>Mar 23 09:57:40 dnsmasq[1952]: started, version 1.18 cachesize 20

Figure 205

Label	Function
Name	Shows the name of the DNS server if not assigned by the Internet service provider.
IP Address	Shows the IP address of the DNS server if not assigned by the Internet service provider.
Systemloggings	Shows the individual operations executed by the DNS server.

21.8 Status – DynDNS

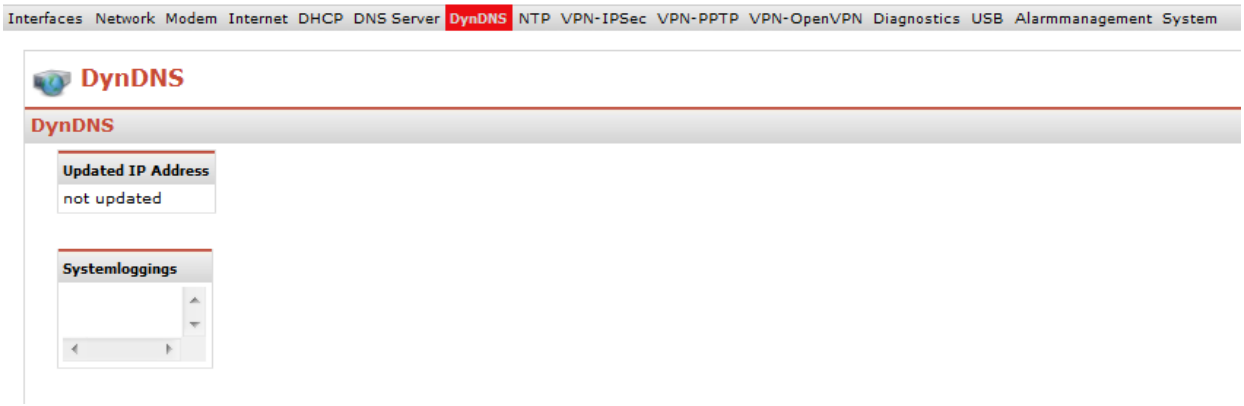

Interfaces Network Modem Internet DHCP DNS Server DynDNS NTP VPN-IPSec VPN-PPTP VPN-OpenVPN Diagnostics USB Alarmmanagement System
DynDNS
DynDNS
Updated IP Address
not updated
Systemloggings

Figure 206

Label	Function
Updated IP Address	Shows the current IP address assigned to the router via the Internet.
Systemloggings	Shows all events and faults related to the DynDNS service.

21.9 Status – NTP

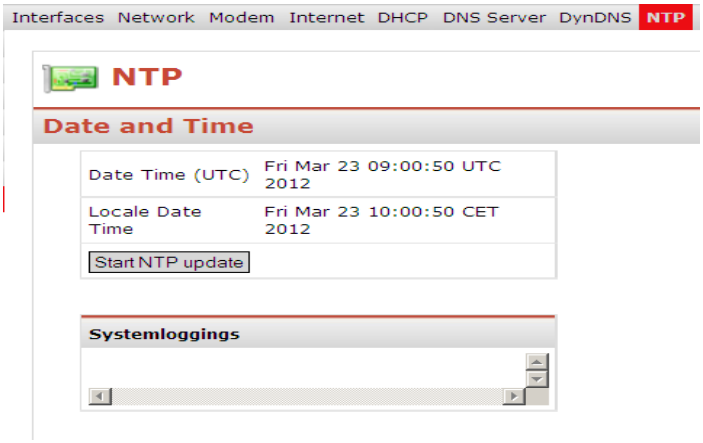


Figure 207

Label	Function
Date Time (UTC)	Shows the current system time in Universal Time Coordinates (UTC).
Local Date Time	Shows the time using the time zone setting.
Systemloggings	Shows all notifications and error messages related to the service.

21.10 Status – VPN-IPSEC

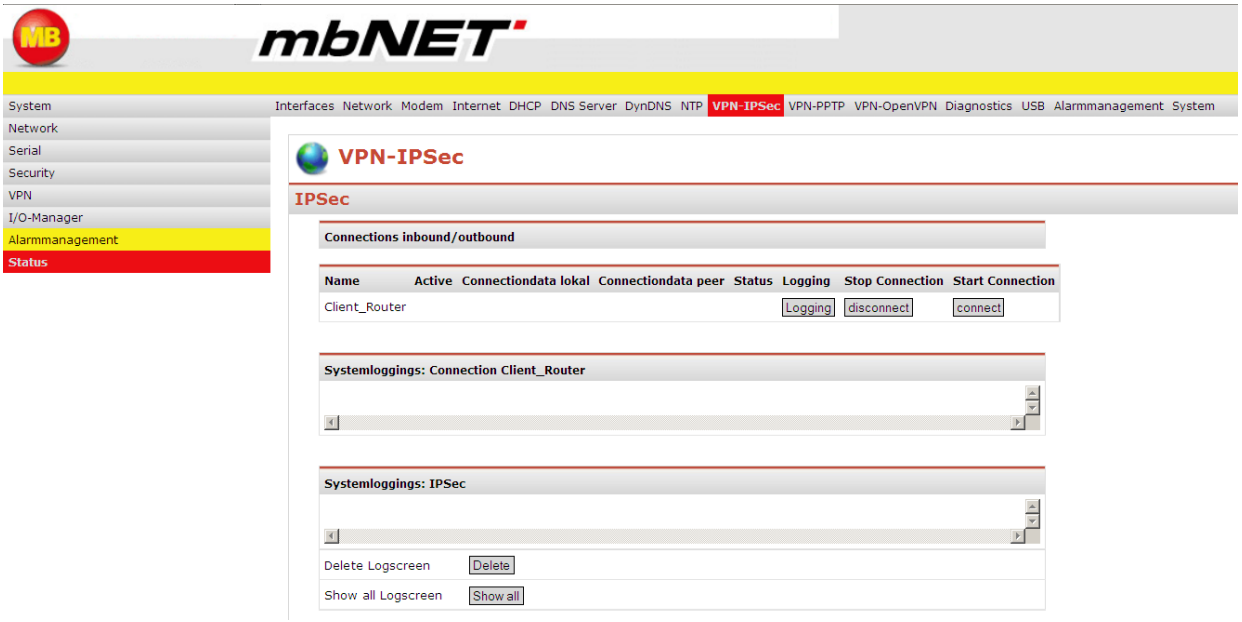


Figure 208

Label	Function
Connections in-bound/outbound	Shows both the incoming and outgoing VPN connections of the router. An active connection is indicated by a green dot. The connection duration and active user are displayed. After the connection is disconnected, the active connection time is displayed. You can manually connect or disconnect the connection here also. **However it is not recommended to use these buttons unless requested to do so by a member of the support team.**

21.11 Status – VPN-PPTP

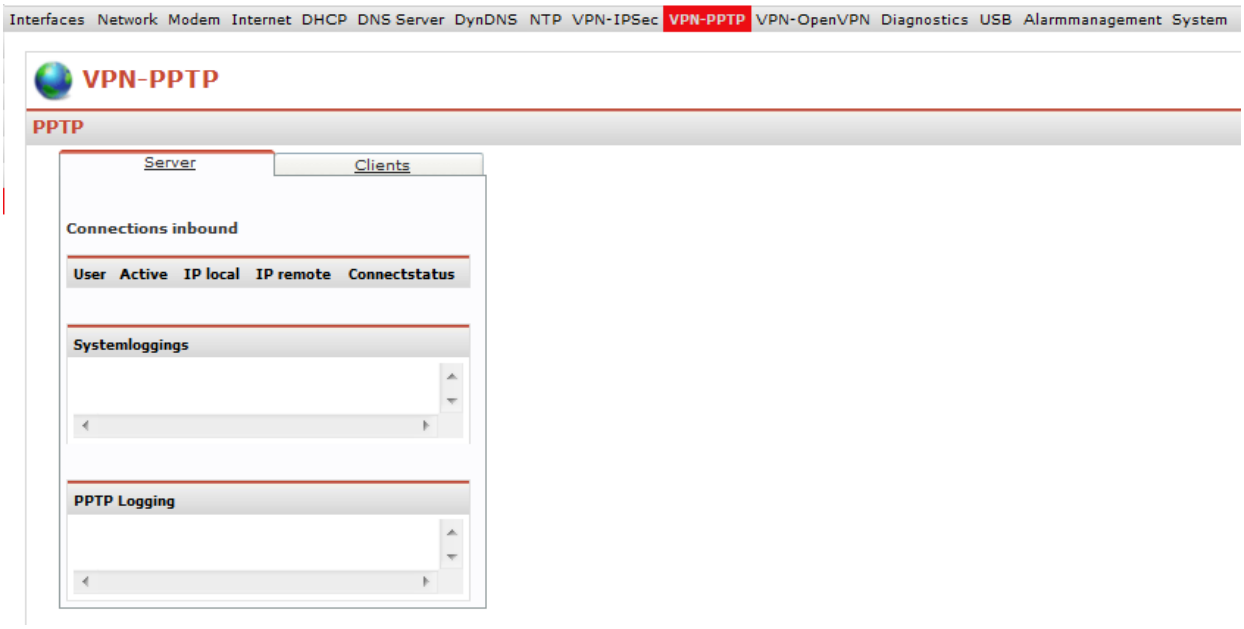


Figure 209

Label	Function
Server	The incoming VPN connections of the router are listed here. An active connection is indicated by a green dot. The connection duration, active user, local and remote IP address are displayed. After the connection is disconnected, you can read off the active connection time.
Clients	Shows the outgoing VPN connections of the router. An active connection is indicated by a green dot. The connection duration, active user, local and remote IP address are displayed. The connections are logged. After the connection is disconnected, you can read off the active connection time.
Systemloggings: Connection	Shows all notifications and error messages related to the PPTP service.

21.12 Status – VPN OpenVPN

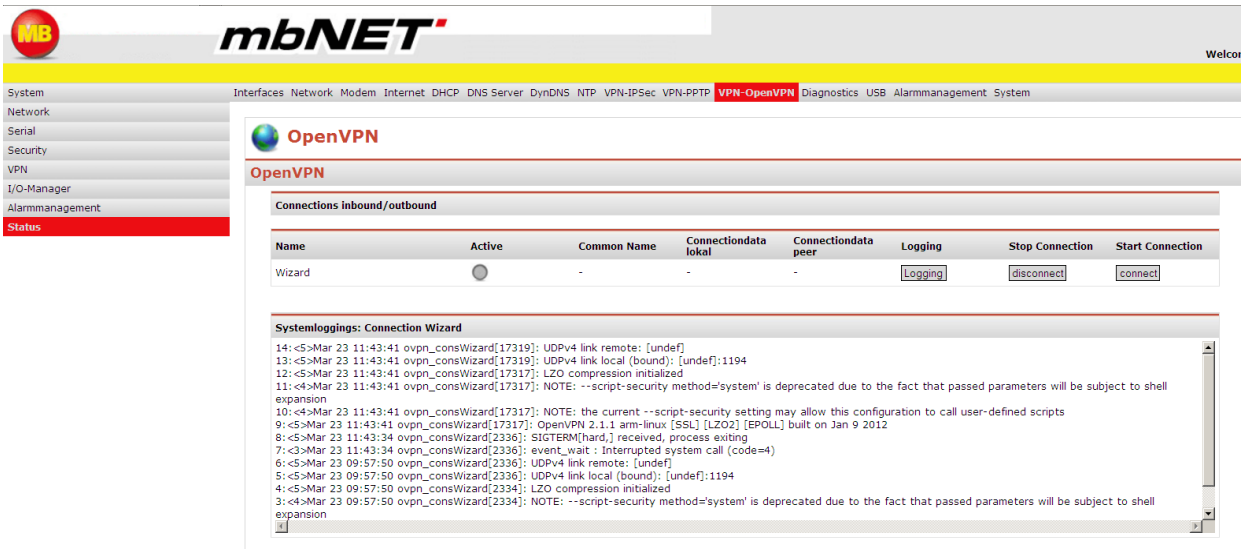

mbNET
Welcor
System
Network
Serial
Security
VPN
I/O-Manager
Alarmmanagement
Status
Interfaces Network Modem Internet DHCP DNS Server DynDNS NTP VPN-IPSec VPN-PPTP VPN-OpenVPN Diagnostics USB Alarmmanagement System
OpenVPN
OpenVPN
Connections inbound/outbound
Name Active Common Name Connectiondata lokal Connectiondata peer Logging Stop Connection Start Connection
Wizard - - - Logging disconnect connect
Systemloggings: Connection Wizard
14:<5>Mar 23 11:43:41 ovpn_consWizard[17319]: UDPv4 link remote: [undef]
13:<5>Mar 23 11:43:41 ovpn_consWizard[17319]: UDPv4 link local (bound): [undef]:1194
12:<5>Mar 23 11:43:41 ovpn_consWizard[17317]: LZO compression initialized
11:<4>Mar 23 11:43:41 ovpn_consWizard[17317]: NOTE: --script-security method='system' is deprecated due to the fact that passed parameters will be subject to shell expansion
10:<4>Mar 23 11:43:41 ovpn_consWizard[17317]: NOTE: the current --script-security setting may allow this configuration to call user-defined scripts
9:<5>Mar 23 11:43:41 ovpn_consWizard[17317]: OpenVPN 2.1.1 arm-linux [SSL] [LZO2] [EPOLL] built on Jan 9 2012
8:<5>Mar 23 11:43:34 ovpn_consWizard[2336]: SIGTERM[hard,] received, process exiting
7:<3>Mar 23 11:43:34 ovpn_consWizard[2336]: event_wait : Interrupted system call (code=4)
6:<5>Mar 23 09:57:50 ovpn_consWizard[2336]: UDPv4 link remote: [undef]
5:<5>Mar 23 09:57:50 ovpn_consWizard[2336]: UDPv4 link local (bound): [undef]:1194
4:<5>Mar 23 09:57:50 ovpn_consWizard[2334]: LZO compression initialized
3:<4>Mar 23 09:57:50 ovpn_consWizard[2334]: NOTE: --script-security method='system' is deprecated due to the fact that passed parameters will be subject to shell expansion

Figure 210

Label	Function
Connections inbound/outbound	Shows both the incoming and outgoing VPN connections of the router. An active connection is indicated by a green dot. The name, local address and peer address are displayed here. You can manually connect or disconnect the connection here also. **However it is not recommended to use these buttons unless requested to do so by a member of the support team.**

21.13 Status – Diagnostics

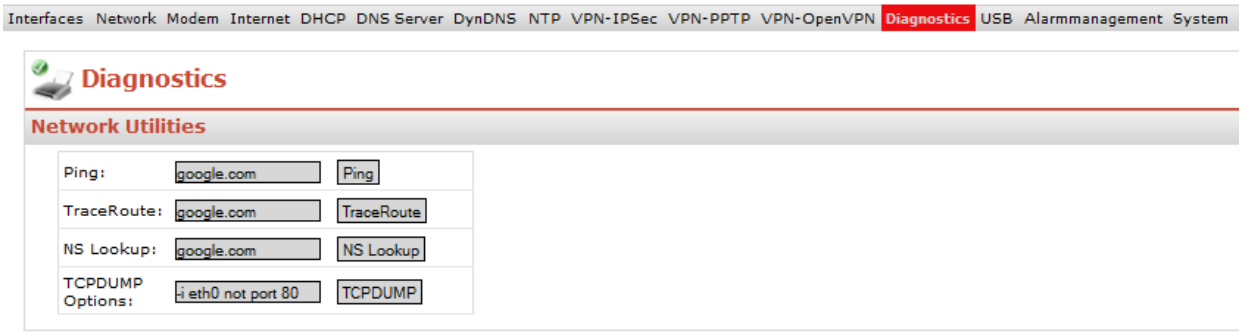

Interfaces Network Modem Internet DHCP DNS Server DynDNS NTP VPN-IPSec VPN-PPTP VPN-OpenVPN Diagnostics USB Alarmmanagement System
Diagnostics
Network Utilities
Ping: google.com Ping
TraceRoute: google.com TraceRoute
NS Lookup: google.com NS Lookup
TCPDUMP Options: -i eth0 not port 80 TCPDUMP

Figure 211

Label	Function
Ping	After an Internet address or IP address is entered, the ping command can determine whether the address in question can be reached. This is e.g. an easy way of determining whether there is an Internet connection active.
TraceRoute	This command provides more information about the network connection between the router and a remote or other computer. It traces and displays the route.
NS Lookup	This function can be used to check whether name resolution (http://www.mbconnectline.de = 88.12.12.34) takes place. If this function ends in an error message, check whether there is a DNS server address under *Network DNS* in your mbNET or whether your network's DNS server is available.

21.14 Status – USB

Interfaces Network Modem Internet DHCP DNS Server DynDNS NTP VPN-IPSec VPN-PPTP VPN-OpenVPN Diagnostics USB Alarmmanagement System
USB Devices
All connected devices (excluding system hubs)
Vendor Model Type Version
Mounted USB / SCSI devices

Figure 212

Label	Function
Shows all connected devices (connected system hubs).	The manufacturer, model, type and version are displayed for connected USB storage media.
Mounted USB / SCSI devices	Shows how the USB storage medium is integrated in the router's file system and the file system created on the USB storage medium.

21.15 Status – Alarmmanagement

Interfaces Network Modem Internet DHCP DNS Server DynDNS NTP VPN-IPSec VPN-PPTP VPN-OpenVPN Diagnostics USB Alarmmanagement System
Input/Output
Input
Input 1 Input 2 Input 3 Input 4
Output
Output 1 Output 2
Messages
Systemloggings

Figure 213

Label	Function
Input	Shows the states at the four inputs. The states are queried and updated approx. every three seconds.
Output	Shows the states at the two outputs. The states are queried and updated approx. every three seconds.
Systemloggings	All events and error messages related to alarm management are saved here (e.g. SMS, activity of inputs).

21.16 Status – System

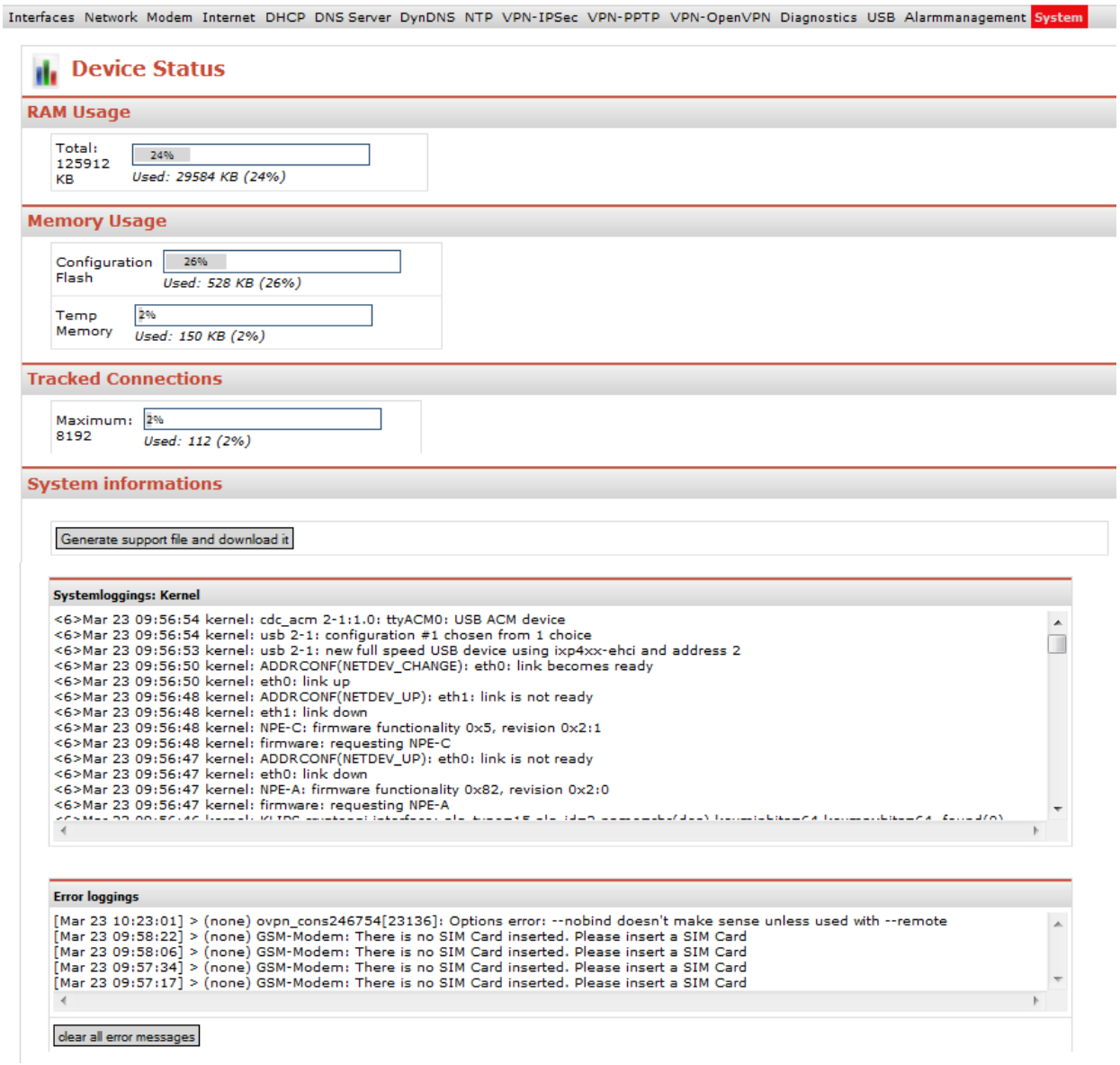

Interfaces Network Modem Internet DHCP DNS Server DynDNS NTP VPN-IPSec VPN-PPTP VPN-OpenVPN Diagnostics USB Alarmmanagement System
Device Status
RAM Usage
Total: 125912 KB
24%
Used: 29584 KB (24%)
Memory Usage
Configuration Flash
26%
Used: 528 KB (26%)
Temp Memory
2%
Used: 150 KB (2%)
Tracked Connections
Maximum: 8192
2%
Used: 112 (2%)
System informations
Generate support file and download it
Systemloggings: Kernel
<6>Mar 23 09:56:54 kernel: cdc_acm 2-1:1.0: ttyACM0: USB ACM device
<6>Mar 23 09:56:54 kernel: usb 2-1: configuration #1 chosen from 1 choice
<6>Mar 23 09:56:53 kernel: usb 2-1: new full speed USB device using ixp4xx-ehci and address 2
<6>Mar 23 09:56:50 kernel: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
<6>Mar 23 09:56:50 kernel: eth0: link up
<6>Mar 23 09:56:48 kernel: ADDRCONF(NETDEV_UP): eth1: link is not ready
<6>Mar 23 09:56:48 kernel: eth1: link down
<6>Mar 23 09:56:48 kernel: NPE-C: firmware functionality 0x5, revision 0x2:1
<6>Mar 23 09:56:48 kernel: firmware: requesting NPE-C
<6>Mar 23 09:56:47 kernel: ADDRCONF(NETDEV_UP): eth0: link is not ready
<6>Mar 23 09:56:47 kernel: eth0: link down
<6>Mar 23 09:56:47 kernel: NPE-A: firmware functionality 0x82, revision 0x2:0
<6>Mar 23 09:56:47 kernel: firmware: requesting NPE-A
Error loggings
[Mar 23 10:23:01] > (none) ovpn_cons246754[23136]: Options error: --nobind doesn't make sense unless used with --remote
[Mar 23 09:58:22] > (none) GSM-Modem: There is no SIM Card inserted. Please insert a SIM Card
[Mar 23 09:58:06] > (none) GSM-Modem: There is no SIM Card inserted. Please insert a SIM Card
[Mar 23 09:57:34] > (none) GSM-Modem: There is no SIM Card inserted. Please insert a SIM Card
[Mar 23 09:57:17] > (none) GSM-Modem: There is no SIM Card inserted. Please insert a SIM Card
clear all error messages

Figure 214

Label	Function
RAM Usage	Shows the amount of RAM memory currently being used by the router.
Memory Usage	Shows the amount of configuration memory and temporary memory currently being used.
Tracked Connections	Shows the usage of the packet filter.
System information	The system information can be used to establish the cause of errors on the router. If, for example, the ERROR LED on the front is flashing, it may be possible to determine the cause of the error using the log.

Error loggings	Firmware versions 2.1.0 and higher feature a direct error logging function in the web interface. This function logs all of the errors until the "clear all error messages" button is clicked. The most recent error is also displayed on the *system information* page and the *wizards page*. Simply click the last error message to go from one of these two pages directly to the error memory.

22. Factory settings on delivery

22.1 Username and password

The router is shipped with the following username and password:

Username: admin

Password: No password required

22.2 IP address of the router

The router is set to the following IP address in the factory:

IP address: 192.168.0.100

23. Loading the factory settings

Follow the steps outlined below to reset the industrial router to the factory settings:

IMPORTANT: You should first **back up** your configuration. Once you have carried out these steps, your previous settings will no longer be available.

1. Switch on the device
2. Wait until the **Err** LED is **on**
3. Press and hold the dial-out button until the **Fc4** / TxD2 LED lights up
4. Press the dial-out button again (**Fc3** / RxD2 lights up)
5. Press the dial-out button again (**Fc2** / TxD1 lights up)
6. Finally press the dial-out button one last time

The custom configuration is then deleted, the industrial router is reset to the factory settings and can be reconfigured.

IMPORTANT: The IP address of the industrial router is reset to 192.168.0.100. The computer's network settings must be changed accordingly.

24. Initializing the modem

General information on the AT commands

The commands can be entered in the input interface (modem settings) in the two fields "Modem Initialization".

The **prefix** always consists of the letters **"AT".**
This does not have to be entered in the field.

The **command** consists of individual characters that are written as described below. It is made up of a code and, if applicable, any associated values.

Letters can be in uppercase and lowercase. Multiple commands can be combined into a command line.

Example: L1M1\N5

24.1 Analog modem commands

B **Selects the communication standard**

ATB0 CCITT modulation
ATB1 Bell modulation

\B **Treatment of the break signal**

AT\Bn Send break signal to remote station
n= 0-9 in 100 ms units (AT\B3 standard)
Only possible with a non-error corrected connection

%C **Data compression setting**

AT%C0 Data compression inactive
AT%C1 Data compression active

+GCI **Country-specific setting**

This command configures the analog modem to the country-specific setting
Example +GCI=B5

Initializing the modem (continued)

L **Loudspeaker volume**

ATL0,1 Low volume
ATL2 Medium volume
ATL3 High volume

M **Loudspeaker mode**

ATM0 Loudspeaker always on
ATM1 Loudspeaker on until data carrier signal is detected
ATM2 Loudspeaker on when the modem is ready to dial
ATM3 Loudspeaker off while the number is being dialed and then, after dialing, until a data carrier signal is detected

+MS **Selects the modulation type**

This command sets the modulation type and the bit rates negotiated between the local and remote modems.
Syntax:
+MS=[<carrier>[,<automode>[,<min_tx_rate>[,<max_tx_rate>[,<min_rx_rate>[,<max_rx_rate>]]]]]

Example: AT+MS= V34,1,9600,33600,9600,33600

Modulation	<carrier>	Possible baud rates
Bell 103	B103	300
Bell 212	B212	1200 Rx 75 Tx or 75 Rx/1200 Tx
V.21	V21	300
V.22	V22	1200
V.22 through	V22B	1200, 2400
V.23	V23C	1200
V.32	V32	4800, 9600
V.32 through	V32B	4800, 7200, 9600, 12000, 14400
V.34	V34	2400, 4800, 7200, 9600, 12000, 14400, 16800, 19200, 21600, 24000, 26400, 28800, 31200, 33600

Automode 0=disabled
1=enabled (default)

AT+MS? Shows the current setting

\N **Selects the error correction settings**

AT\N0 Error correction switched off
AT\N1 Transparent transmission of any data widths via the serial interface, without data buffering and error correction.
AT\N2 V.42LAP-M or MNP 4 error correction. The modem hangs up if a failsafe connection cannot be established.
AT\N3 V.42LAP-M or MNP 4 error correction. A non-failsafe connection will be attempted if a failsafe connection cannot be established.
AT\N4 V.42LAP-M error correction; the modem hangs up if this is not possible.
AT\N5 MNP error correction; the modem hangs up if this is not possible.

Initializing the modem (continued)

X **Message output, dial tone detection**

This command controls how the modem reacts to the dial tone and busy signal and how it displays the CONNECT messages.

ATX0 No busy and dial tone detection
i.e. NO CARRIER is displayed in response to a failed dialing attempt.
Messages: OK, CONNECT, RING, NO CARRIER, ERROR and NO ANSWER are displayed
ATX1 Like ATX0 but CONNECTxxx messages with speed specification
ATX2 Busy tone detection disabled, dial tone detection enabled
Messages: OK, CONNECT, RING, NO CARRIER, ERROR, NO ANSWER and NO DIAL TONE are displayed
ATX3 Busy tone enabled, dial tone detection disabled
Messages: OK, CONNECT xxx, RING, NO CARRIER, ERROR, NO ANSWER
ATX4 Busy tone and dial tone detection enabled
Messages: OK, CONNECTxxx, RING, NO CARRIER, ERROR, NO ANSWER and NO DIAL TONE

24.2 ISDN terminal adapter (TA) commands

B **Defines the transmission protocol in the B channel**

ATB0: V.110 asynchronous
ATB3: PPP asynchronous to synchronous conversion (PPP asynchronous single link)
ATB4: HDLC transparent
ATB5: Byte transparent (B channel data)
ATB10: X.75 transparent
ATB13: V.120
ATB20: X.31 B channel (X.25 B channel)
ATB21: X.31 D channel

N **Defines the transmission rate in V.110 mode**

ATN0 Automatic connection speed
ATN1 Connection speed 1,200 bps
ATN2 Connection speed 2,400 bps
ATN3 Connection speed 4,800 bps
ATN4 Connection speed 9,600 bps
ATN5 Connection speed 19,200 bps

#Z **Defines the MSN (multiple subscriber number)**
All calls are accepted if the number is set to "*" (asterisk) (default setting).
An MSN generally has to be entered as this is required by most PBX systems. The MSN must also be enabled for the data service.

AT#Z=n Sets MSN to n

25. Appendix

25.1 Country codes for analog devices

No.	Country	Modem operation setting
1	Afghanistan	B5
2	Albania (AL)	B5
3	Algeria (DZ)	B5
4	American Samoa (AS)	B5
5	Andorra (AD)	B5
6	Angola (AO)	B5
7	Anguilla (AI)	B5
8	Antarctica (AQ)	B5
9	Antigua and Barbuda (AG)	B5
10	Argentina (AR)	07
11	Armenia (AM)	B5
12	Aruba (AW)	B5
13	Australia (AU)	09
14	Austria (AT)	FD
15	Azerbaijan (AZ)	B5
16	Bahamas, The (BS)	B5
17	Bahrain (BH)	B5
18	Bangladesh (BD)	B5
19	Barbados (BB)	B5
20	Belarus (BY)	B5
21	Belgium (BE)	FD
22	Belize (BZ)	B5
23	Benin (BJ)	B5
24	Bermuda (BM)	B5
25	Bhutan (BT)	B5
26	Bolivia (BO)	B5
27	Bosnia and Herzegovina (BA)	B5
28	Botswana (BW)	B5
29	Bouvet Island (BV)	B5
30	Brazil (BR)	16
31	British Indian Ocean Territory (IO)	B5
32	Brunei (BN)	B5
33	Bulgaria (BG)	FD
34	Burkina Faso (BF)	B5
35	Burundi (BI)	B5
36	Cambodia (KH)	B5
37	Cameroon (CM)	B5
38	Canada (CA)	B5
39	Cape Verde (CV)	B5
40	Cayman Islands (KY)	B5
41	Central African Republic (CF)	B5
42	Chad (TD)	B5
43	Chile (CL)	B5
44	China (CN)	B5
45	Christmas Island (CX)	B5

No.	Country	Modem operation setting
46	Cocos (Keeling) Islands (CC)	B5
47	Colombia (CO)	B5
48	Comoros (KM)	B5
49	Congo (CG)	B5
50	Cook Islands (CK)	B5
51	Costa Rica (CR)	B5
52	Cote D'Ivoire (CI)	B5
53	Croatia (HR)	B5
54	Cuba (CU)	B5
55	Cyprus (CY)	FD
56	Czech Republic (CZ)	FD
57	Denmark (DK)	FD
58	Djibouti (DJ)	B5
59	Dominica (DM)	B5
60	Dominican Republic (DO)	B5
61	East Timor (TP)	B5
62	Ecuador (EC)	B5
63	Egypt (EG)	B5
64	El Salvador (SV)	B5
65	Equatorial Guinea (GQ)	B5
66	Eritrea (ER)	B5
67	Estonia (EE)	FD
68	Ethiopia (ET)	B5
69	Falkland Islands (Islas Malvinas) (FK)	B5
70	Faroe Islands (FO)	B5
71	Fiji (FJ)	B5
72	Finland (FI)	FD
73	France (FR)	FD
74	France, Metropolitan (FX)	FD
75	French Guiana (GF)	B5
76	French Polynesia	B5
77	French Southern Territories (TF)	B5
78	Gabon (GA)	B5
79	Gambia, The (GM)	B5
80	Georgia (GE)	B5
81	Germany (DE)	FD
82	Ghana (GH)	B5
83	Gibraltar (GI)	B5
84	Greece (GR)	FD
85	Greenland (GL)	B5
86	Grenada (GD)	B5
87	Guadeloupe (GP)	B5
88	Guam (GU)	B5
89	Guatemala (GT)	B5
90	Guinea (GN)	B5
91	Guinea-Bissau (GW)	B5
92	Guyana (GY)	B5
93	Haiti (HT)	B5
94	Heard Island and McDonald Islands (HM)	B5

No.	Country	Modem operation setting
95	Honduras (HN)	B5
96	Hong Kong (HK)	99
97	Hungary (HU)	FD
98	Iceland (IS)	FD
99	India (IN)	B5
100	Indonesia (ID)	99
101	Iran (IR)	B5
102	Iraq (IQ)	B5
103	Ireland (IE)	FD
104	Israel (IL)	B5
105	Italy (IT)	FD
106	Jamaica (JM)	B5
107	Japan (JP)	00
108	Jordan (JO)	B5
109	Kazakhstan (KZ)	B5
110	Kenya (KE)	B5
111	Kiribati (KI)	B5
112	Korea, Democratic People's Republic of (KP)	B5
113	Korea, Republic of (KR)	B5
114	Kuwait (KW)	B5
115	Kyrgyzstan (KG)	B5
116	Lao People's Democratic Republic (LA)	B5
117	Latvia (LV)	FD
118	Lebanon (LB)	B5
119	Lesotho (LS)	B5
120	Liberia (LR)	B5
121	Libya (LY)	B5
122	Liechtenstein (LI)	FD
123	Lithuania (LT)	FD
124	Luxembourg (LU)	FD
125	Macau (MO)	B5
126	Macedonia (MK)	B5
127	Madagascar (MG)	B5
128	Malawi (MW)	B5
129	Malaysia (MY)	6C
130	Maldives (MV)	B5
131	Mali (ML)	B5
132	Malta (MT)	FD
133	Marshall Islands (MH)	B5
134	Martinique (MQ)	B5
135	Mauritania (MR)	B5
136	Mauritius (MU)	B5
137	Mayotte (YT)	B5
138	Mexico (MX)	B5
139	Micronesia, Federated States of (FM)	B5
140	Moldova, Republic of (MD)	B5
141	Monaco (MC)	B5
142	Mongolia (MN)	B5
143	Montserrat (MS)	B5

No.	Country	Modem operation setting
144	Morocco (MA)	B5
145	Mozambique (MZ)	B5
146	Myanmar (MM)	B5
147	Namibia (NA)	B5
148	Nauru (NR)	B5
149	Nepal (NP)	B5
150	Netherlands (NL)	FD
151	Netherlands Antilles (AN)	FD
152	New Caledonia (NC)	B5
153	New Zealand (NZ)	7E
154	Nicaragua (NI)	B5
155	Niger (NE)	B5
156	Nigeria (NG)	B5
157	Niue (NU)	B5
158	Norfolk Island (NF)	B5
159	Northern Mariana Islands (MP)	B5
160	Norway (NO)	FD
161	Oman (OM)	B5
162	Pakistan (PK)	B5
163	Palau (PW)	B5
164	Panama (PA)	B5
165	Papua New Guinea (PG)	B5
166	Paraguay (PY)	B5
167	Peru (PE)	B5
168	Philippines (PH)	B5
169	Pitcairn Islands (PN)	B5
170	Poland (PL)	FD
171	Portugal (PT)	FD
172	Puerto Rico (PR)	B5
173	Qatar (QA)	B5
174	Reunion (RE)	B5
175	Romania (RO)	FD
176	Russian Federation (RU)	B5
177	Rwanda (RW)	B5
178	St. Helena (SH)	B5
179	Saint Kitts and Nevis (KN)	B5
180	Saint Lucia (LC)	B5
181	St. Pierre and Miquelon (PM)	B5
182	Saint Vincent and the Grenadines (VC)	B5
183	Samoa (WS)	B5
184	San Marino (SM)	B5
185	Sao Tome and Principe (ST)	B5
186	Saudi Arabia (SA)	B5
187	Senegal (SN)	B5
188	Seychelles (SC)	B5
189	Sierra Leone (SL)	B5
190	Singapore (SG)	9C
191	Slovakia (SK)	FD
192	Slovenia (SI)	FD

No.	Country	Modem operation setting
193	Solomon Islands (SB)	B5
194	Somalia (SO)	B5
195	South Africa (ZA)	9F
196	South Georgia and South Sandwich Islands (GS)	B5
197	Spain (ES)	FD
198	Sri Lanka (LK)	B5
199	Sudan (SD)	B5
200	Suriname (SR)	B5
201	Svalbard and Jan Mayen Islands (SJ)	B5
202	Swaziland (SZ)	B5
203	Sweden (SE)	FD
204	Switzerland (CH)	FD
205	Syrian Arab Republic (SY)	B5
206	Taiwan (TW)	FE
207	Tajikistan (TJ)	B5
208	Tanzania, United Republic of (TZ)	B5
209	Thailand (TH)	B5
210	Togo (TG)	B5
211	Tokelau (TK)	B5
212	Tonga (TO)	B5
213	Trinidad and Tobago (TT)	B5
214	Tunisia (TN)	B5
215	Turkey (TR)	FD
216	Turkmenistan (TM)	B5
217	Turks and Caicos Islands (TC)	B5
218	Tuvalu (TV)	B5
219	Uganda (UG)	B5
220	Ukraine (UA)	B5
221	United Arab Emirates (AE)	B5
222	United Kingdom (UK)	FD
223	United States (US)	B5
224	United States Minor Outlying Islands (UM)	B5
225	Uruguay (UY)	B5
226	Uzbekistan (UZ)	B5
227	Vanuatu (VU)	B5
228	Vatican City State (Holy See) (VA)	B5
229	Venezuela (VE)	B5
230	Vietnam (VN)	99
231	Virgin Islands (British) (VG)	B5
232	Virgin Islands (U.S.) (VI)	B5
233	Wallis and Futuna Islands (WF)	B5
234	Western Sahara (EH)	B5
235	Yemen (YE)	B5
236	Yugoslavia (YU)	B5
237	Zaire (ZR)	B5
238	Zambia (ZW)	B5
239	Zimbabwe (ZW)	B5

26. Index

A

Alarm management 197

B

Basic configuration 25
Brief description 8
Buttons 23

C

Connection Scenarios 29
Connection status 39

D

Default password 21
Digital outputs 201
Displays, controls and connections 12

F

Factory settings on delivery 221
Features 8
Fields 23
Firewall 150
First time operation 17
Forwarding 154

G

Grounding conductor 17

H

Home page 22
How to set computer address (IP address) and subnet mask 20

I

Icons 23
Initial configuration 21
Initializing the modem 222
Interfaces 15

L

LAN>WAN 152

N

NAT 155
Network – DHCP 125
Network – DNS server 126
Network – DynDNS 128
Network – Hosts 127
Network – Internet 119
Network – LAN 108
Network – Modem 110
Network – WAN 109

P

Password 221
Pin assignment 15

S

Safety instructions 9
Save Settings 28
Security settings 150, 151, 155
Security Settings 27
Serial interfaces 131
Status – Alarmmanagement 218
Status – DHCP 209
Status – Diagnostics 215, 216
Status – DNS Server 210
Status – DynDNS 211
Status – Interfaces 202
Status – Internet 207
Status – Modem 205
Status – Network 204
Status – NTP 212
Status – System 219
Status – USB 217
Status – VPN-IPSEC 213
Status – VPN-PPTP 214
Status messages (extract) 202
System – Certificates 98, 99, 100, 101, 102
System – Configuration 105
System – Firmware 106
System – Logging 104
System – USB 103
System – WEB 93
System settings 25

T

Technical data 10

U

Username and password 221
Username: 221

V

VPN connection 58

W

WAN>LAN 151
Web interface 22
What is included in the package 11